PROYECTO FIN DE CARRERA

"Uso de la norma ISO/IEC 27004 para Auditoría Informática"

INGENIERIA TECNICA DE INFORMATICA DE GESTION

Autor: AGUSTÍN LARRONDO QUIRÓS NIA: 100061619

Tutor: MIGUEL ÁNGEL RAMOS

Leganés octubre de 2010.

Título: Uso de la norma ISO/IEC 27004 para Auditoría Informática.

Autor: AGUSTÍN LARRONDO QUIRÓS

Director: MIGUEL ÁNGEL RAMOS

EL TRIBUNAL

Presidente: BENJAMÍN RAMOS

Vocal: FUENSANTA MEDINA DOMÍNGUEZ

Secretario: EDUARDO GALÁN HERRERO

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 14 de Octubre de 2010 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

A mi profesor Miguel Ángel Ramos por ayudarme a hacer este proyecto con su indispensable apoyo, estando siempre y ayudándome a resolver las dudas que surgían en cualquier momento del día. Pocos profesores he conocido así.

A todos mis abuelos Agustín, Rafael, Orencia y Visitación, los cuales sepan donde quieran que estén, que ya tienen a su primer ingeniero en la familia y que deseo y espero no ser el último.

A mis padres Fernando y Rosario, darles las gracias por darme la oportunidad de permitirme estudiar una carrera, sobre todo cuando ellos no han tenido esa oportunidad en sus vidas, así como de ofrecerme su plena confianza en mí para conseguirla, por todos los besos y abrazos que me dieron, así como por aguantarme en mis buenos como en mis malos momentos durante estos años de carrera, ya que sin ellos esto no sería posible. GRACIAS.

A mis hermanos Rafael y Fernando, también conocido el primero como RAFA y el segundo como NANETE o NANO, ambos me enseñaron a no rendirme ante la adversidad, por sus consejos, por apoyarme en los malos momentos, por esas partidas a la play, por ese baño en su piscina, por ese viaje de sky el cual necesitaba y por todos los abrazos que me dieron durante años. Gracias por estar a mi lado.

A mi amigo David conocido también como Tejero o Tejerito, por sus "amenazas" que recibía para seguir estudiando la carrera cada vez que le decía que no sería capaz de terminarla, por todas esas partidas a los dardos, por hacerme reír tanto en los buenos momentos como en los malos, y por esa energía positiva que transmite a la gente que le rodea.

A mi amiga Eva o Evita, por todas esas noches cenando o de copas por Getafe o por Madrid, en las cuales siempre "esta chiquilla" me esperaba con un abrazo, un beso y una sonrisa independientemente de cómo se encontraba ella para animarme y poder hablar cuando lo necesitaba. Tengo que apreciar siempre esos buenos detalles.

A mis amigos Rubén y Lorenzo conocidos también como LOS GEMELOS, por esas noches “perdidas” entre risas y chupitos de tequila por Getafe, en las cuales no sabíamos dónde íbamos a terminar pero sí con quien las estábamos pasando. Gracias por esas noches!

A mi amiga Sonia, por esas noches de terrazas de verano, sus abrazos y por enseñarme que los museos no son tan aburridos después de todo. “¡Debería estar en un museo!" Sigue estudiando chiquilla, tu puedes!

A mi amigo Rubén, por todas esas palizas que recibí en la play, por aguantarme en mis días más críticos en los cuales me volvía insoportable, por enseñarme el camino de la palabra y lo más importante, a estar presente cuando necesitaba hablar. Hay que saber valorar esas pequeñas cosas.

A mi amigo Juan Carlos, por todas esas noches de fiesta “…paseando por donde los garitos...” ya sea Madrid, Getafe, Benidorm, Salou, etc. Por esas terrazas de verano con sus múltiples conversaciones. Sin ti a la noche le falta algo y no se puede salir de juerga. Va a ser LEGENDARIO!!

A mi amigo Diego, por aguantarme en mis días malos, por sus conocimientos aportados en estos años de carrera, por esos largos paseos por parquesur, por sus comentarios graciosos sobre series de televisión y videojuegos, hacía las clases más llevaderas.

A mi amigo Oscar, por sus conocimientos sobre chistes, por apoyarme en los buenos momentos como en los malos, por las múltiples conversaciones en la cafetería de la universidad tomando café y por ese viaje terminando en un hotel perdido de la mano de Dios sacado de una película de terror.

A mi amiga Paula, por todas esas noches de bolos, maquinas de bailar, cenas, conversaciones, cines y algún que otro bingo y/o chupito de piruleta por ahí perdido. Habrá que repetirlo chiquilla.

Y a los amigos que dejamos atrás, por diversos motivos, que aún así también pusieron su granito de arena.

En resumen, a todos ellos por enseñarme a creer en mí mismo. Y por todas esas charlas que tuvimos a lo largo de los años en cualquier momento del día y de la noche.

Solo puedo decir, que soy la suma de todos vuestros apoyos, gracias por todo y os deseo lo mejor en vuestras vidas.

Para finalizar quiero concluir con una frase que siempre me ha gustado escucharla y por tanto quiero añadirla.

"¿Por qué nos caemos?

Para aprender a levantarnos."

P.D.: Esta noche invito yo!!

INDICE

1. INTRODUCCION

Cómo empezar este proyecto resumiendo todo en una frase… “NO PODEMOS CONTROLAR AQUELLO QUE NO SE PUEDE MEDIR” esta frase que parece tan sencilla es el punto central de todo el proyecto, y esto es debido a que, ¿Cómo vamos a saber solucionar los problemas que nos surgen si no sabemos cuál es la gravedad de dicho problema?

Para solucionarlo necesitamos el uso de métricas las cuales nos ayudarán a alcanzar nuestros objetivos de una forma eficaz, rápida, sin errores y lo más importante reduciendo el coste que nos ocasionarían dichos problemas, los cuales surgirán a la hora de realizar nuestro trabajo.

Si nos encontramos ante un control el cual no sabemos cómo medir, aquí seria donde entraría el estándar ISO/IEC 27004, el cual nos proporciona la ayuda necesaria para realizar dicha medición.

La norma ISO/IEC 27004 comienza con una pequeña introducción, en la que cabe destacar lo siguiente, para aclarar en qué consiste:

“This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved. It needs to be kept in mind that no measurement of controls can guarantee complete security.”

Traduciéndolo al español:

“Esta norma Internacional proporciona orientación sobre la elaboración y utilización de medidas y la medición para evaluar la eficacia de un sistema de gestión de la información aplicadas de seguridad (SGSI) y controles o grupos de controles, tal como se especifica en la norma ISO/IEC 27001.

Esto incluye la política, gestión de información de riesgo de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su revisión, ayudar a determinar si alguno de los procesos de SGSI o controles necesitan ser cambiados o mejorados. Hay que tener en cuenta que ninguna de las mediciones de los controles puede garantizar la seguridad total.”

Por lo tanto con este proyecto el objetivo es entender mejor la ISO/IEC 27004, además mediante el uso de los cuestionarios nos indicará si estamos realizando correctamente dicha normativa a través de una serie de preguntas, las cuales al ser respondidas nos indicará en qué estado se encuentra la empresa o entidad en la que realiza dicha ISO/IEC 27004.

2. SEGURIDAD INFORMATICA

En este punto hablaremos sobre la seguridad informática y los métodos necesarios con el fin de garantizar dicha seguridad.

3. AUDITORIA INFORMATICA

Aquí nos centraremos en qué consiste, por qué se tiene que hacer y cómo se realiza dicha auditoría.

4. ¿QUE ES UNA ISO/IEC?

Hablaremos sobre qué consiste una normativa, explicaremos por separado en qué consiste la ISO e IEC, así como cuando son ISO/IEC.

5. ¿QUE ES UNA METRICA?

Nos centraremos sobre en qué consiste, como conseguir buenas métricas, su clasificación, etc.

6. ISO/IEC 27004

Trataremos sobre la norma ISO/IEC 27004.

7. CUESTIONARIO-APLICACIÓN

Mostraremos un ejemplo sobre cómo crear un cuestionario.

8. USO DEL CUESTIONARIO

Indicaremos como utilizar un caso de ejemplo de un cuestionario en particular.

9. PREGUNTAS DEL CUESTIONARIO

Mostraremos todas las preguntas realizadas a la hora de la aplicación del cuestionario.

ANEXO

En él veremos los diferentes tipos de auditoría que pueden existir en el mercado laboral, además ayudará como complemento.

2. SEGURIDAD INFORMATICA

2.1 Introducción seguridad informática

Cuando hablamos de seguridad pensamos que es una especie de clase (o estado) donde nuestro equipo informático está libre de cualquier tipo de ataque que pueda ocasionar daños tanto a la infraestructura de nuestra empresa o entidad que puede provocar en el peor de los casos la pérdida de la información necesaria para la empresa.

"*¿Se imaginan bancos en los cuales se pierda la información de nuestras cuentas corrientes, aseguradoras que pierden clientes, hospitales en los cuales se pierdan nuestros registros como pacientes, y todo ello por no tener un mínimo de seguridad? la verdad si eso llegase a ocurrir el mundo sería un completo caos a nivel global.*"

Por tanto para que un sistema pueda estar seguro debe de tener las siguientes principales características las cuales son esenciales para tener seguridad ante posibles errores o ataques que puedan surgir:

Confidencialidad: con esta característica conseguimos que la información que estamos salvaguardando sólo pueda ser legible por parte de los usuarios autorizados e impidiendo que sea legible por terceros.

No Repudio: consiste en que si dicha información es modificada o simplemente ha sido legible por parte de los usuarios autorizados quedará registrado, obteniendo así que el usuario autorizado no podrá negar dicho uso, debido a dicho registro

Integridad: la información que se está salvaguardando solo podrá ser modificada por usuarios autorizados.

Disponibilidad: debe de estar presente en cualquier momento para la utilización de los usuarios.

Además de estas características hay que decir que **no existe la seguridad total,** ya que es una utopía, simplemente lo que podemos hacer es reducir los posibles errores que tenga nuestra seguridad, nadie ni nada nos garantiza la seguridad total, solo podemos saber si nuestra seguridad es alta, media o baja, pero no nos garantiza que puedan existir huecos por los cuales pueda peligrar la información de la entidad.

2.1.1 Quien tiene la información controlará el mundo ¿Por qué?

La información es el centro de poder de la mayoría de entidades, como por ejemplo los bancos, no existe el dinero físico, disminuyen los registros en papel, o por ejemplo las fichas físicas de los historiales de los pacientes de cualquier hospital están siendo transferidas a bases de datos, toda la información está centralizada y tiene un grandísimo valor, al fin al cabo, es lo que aparece en las pantallas de nuestros ordenadores, “son datos”, son nuestra información y sin ella no tenemos absolutamente nada.

Por tanto quien controle dicha información podrá controlar aquello que representa.

Hay que destacar que dicha información que tenemos puede ser robada, modificada y usada en beneficio propio, son estas cosas por las cuales la información debe de estar asegurada de que nunca salga de la entidad y caiga en manos ajenas.

Al fin al cabo la información es poder. Y por tanto es crítica para la entidad ya que a partir de ella se toman decisiones a corto, medio y largo plazo, debe de ser conocida solo por las personas autorizadas de la entidad y por último es totalmente importante ya que es el activo de la empresa, es decir lo es todo.

Además la seguridad de la información se expande desde la identificación de problemas, confidencialidad, integridad, comunicación, análisis de riegos hasta la recuperación de dichos riesgos.

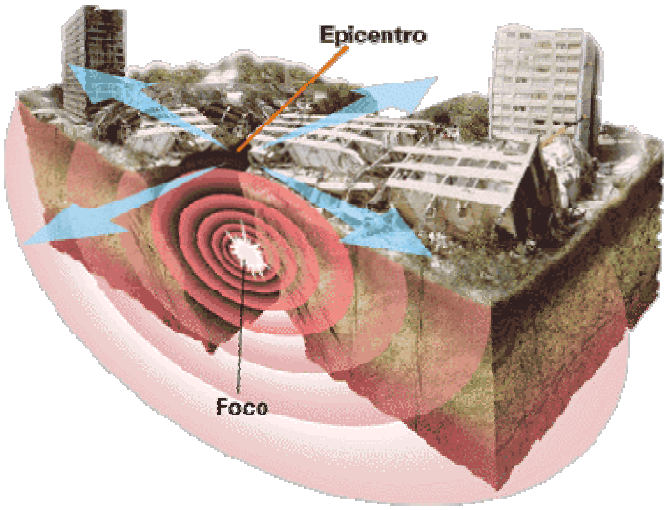
La seguridad de la información tiene como objetivo la protección de los datos y de los sistemas de información de su uso y acceso, que va desde su interrupción, destrucción no autorizada, corrupción o su divulgación.

2.2 Seguridad ambiental

Cuando hablamos de seguridad ambiental nos estamos refiriendo a los procedimientos, procesos y controles con el fin de controlar los efectos de la naturaleza, los cuales pueden dañar seriamente a los equipos informáticos, personal de la entidad y lo más importante los datos de la empresa. Estos efectos de la naturaleza pueden ser: terremotos, inundaciones, fuegos, tormentas eléctricas, picos de tensión, etc.; Los cuales los comentaremos a continuación, así como posibles soluciones para prevenirlos.

2.2.1 Terremotos

Los terremotos o seísmos son una serie de sacudidas del terreno debido al choque entre las placas tectónicas y también a la liberación de energía en el curso de una reorganización brusca de los materiales de la corteza terrestre debido a superar el estado de equilibrio mecánico.



Respecto a la hora de invertir en estas medidas, depende mucho de la situación geográfica de la entidad, por ejemplo, si estuviéramos en un país como Japón donde los terremotos están a la orden del día sería totalmente necesaria y fundamental dicha inversión, pero si fuese como en el caso de España, donde nunca se da ningún terremoto importante ya que sus posibilidades son mínimas dichas inversiones serán menores.

En este caso se recomienda no situar nuestros equipos o sistemas informáticos cerca de las ventanas o en superficies altas por miedo de sus posibles caídas, se recomienda

el uso de fijaciones. Por supuesto tampoco hay que colocar objetos pesados encima de los equipos por miedo a provocar daños en dichos equipos.

También se recomienda el uso de plataformas de goma las cuales absorben parte de las vibraciones generadas por los terremotos, además del uso de mesas anti-vibraciones ya que sin ellas podrían dañar los discos duros donde se guarda la información vital.

2.2.2 Inundaciones

Las inundaciones consisten en la ocupación del agua en zonas que están libres de ella, esto es debido por el desbordamiento de ríos, subida de mareas, o por avalanchas causadas por maremotos.

Estos problemas son graves ya que son los que más daño hacen a la entidad, ya que cualquier sistema eléctrico en contacto con el agua, puede ser mortal para los empleados de la entidad y se perderá toda la última información obtenida además de la pérdida del equipo electrónico ya que dejará de funcionar y no tendrá reparación alguna.

Además nunca habrá que ponerse en contacto físicamente con los equipos electrónicos ya que su contacto sería mortal para los empleados de la entidad.

Se recomienda el uso de detectores de agua los cuales al dispararse la alarma corten automáticamente la corriente eléctrica para evitar males mayores.

Para su detención se recomienda avisar a las autoridades necesarias (bomberos, policía, etc.) con el fin de terminar con dicho problema, ya que tendrán que cortar la corriente eléctrica, en caso de que nuestro sistema de seguridad no haya podido hacerlo. Nunca deberá de hacerlo personal de la entidad.

2.2.3 Fuegos (incendios)

El fuego consiste en una reacción química de una oxidación violenta de una materia combustible, provocando desprendimiento de llamas, vapor de agua, dióxido de carbono y calor. Es un proceso exotérmico.

Los fuegos son ocasionados por cortocircuitos, cigarros mal apagados, etc., y estos ocasionan gravísimos daños tanto materiales como personales.

Se recomienda el uso de alarmas, las cuales al detectar fuego o humo, se activan directamente los extintores que están situados en el techo y avisan a las autoridades con el fin de evitar males mayores.

También es necesario el uso de extintores de mano que estén repartidos por toda la entidad. Además al lado de estos extintores deben existir carteles anunciado su presencia e indicando su situación.

2.2.4 Tormentas eléctricas

Las tormentas eléctricas consisten en fenómenos atmosféricos los cuales pueden ocasionar graves daños físicos a la entidad, estos daños pueden ser desde fuegos ocasionados por las tormentas hasta picos de tensión los cuales pueden destrozar nuestros equipos informáticos con sus respectivos datos.

Se recomienda el uso de pararrayos, estos consisten en una varilla de metal, puesta en el tejado o en la parte más elevada del edificio de la entidad, la cual tiene un cable de cobre que va a aparar a una plancha del mismo metal introducida a unos metros bajo tierra. En caso de que un rayo toque el pararrayos este de descargará al tocar tierra. Evitando posibles daños.

Además se recomienda que las copias de seguridad que se realicen estén siempre alejadas de las estructuras metálicas del edificio de la entidad.

2.2.5 Picos de tensión

Los picos de tensión son otros problemas que puede tener cualquier entidad y consiste en una sobrecarga en la corriente eléctrica, los cuales pueden provocar pequeños daños a nuestros equipos informáticos.

Se recomienda el uso de SAIs, los cuales consisten como dicen sus siglas en un Sistema de Alimentación Ininterrumpida, gracias a estos dispositivos en caso de que exista un pico de tensión mantendrá al equipo en un estado a salvo de cualquier posible daño.

2.2.6 Back Up

Un back Up consiste en una copia de seguridad en formato digital de la documentación de los datos de la entidad, es un conjunto de archivos, los cuales son almacenados con el fin de protegerlos ante cualquier daño interior o exterior a la entidad.

Estas copias de seguridad son útiles, ya que nos sirven para restaurar un equipo informático después de haber ocurrido un ataque, desastre para recuperar archivos que hayan sido borrados sin querer, y la más importante de todas, es que es obligatorio ya que es necesario guardar los datos debido a la AEPD (Agencia Española de Protección de Datos) en relación a los datos personales.

2.3 Seguridad lógica

En este caso cuando llamamos seguridad lógica consiste en que los procedimientos de seguridad sirven para saber quién, cómo y cuando un usuario accede a una parte de la información, por tanto sus procedimientos sirven para controlar dicho acceso lógico, y en caso de que no sea el usuario adecuado para la información, el sistema bloqueará dicha información, para ello incluirá barreras y controles que protejan el acceso de los datos a terceras personas que no tengan la autorización necesaria.

Para ello hay que realizar una serie de puntos clave para la seguridad lógica:

-En caso de problemas en la transmisión debe de haber un proceso de emergencia con el fin de que la información pueda llegar hasta el destinatario.

-Comprobar que los empleados que usen dichos archivos y programas puedan estar trabajando sin necesidad de una supervisión y que a la vez no sean capaces de cambiar o modificar los archivos y programas que no les corresponden como empleados.

-La información recibida por el destinatario, tiene que ser la misma que la que fue enviada desde el origen.

-Limitar el acceso a los archivos y programas de la entidad.

-Sostener que los empleados que están utilizando los archivos, programas y los datos están siendo utilizados en el procedimiento correcto y no por otros.

-Toda la información transferida solo puede ser recibida por el destinario real, y no a terceros, ya que esto sería un grave problema en la entidad.

-Deben de existir diferentes caminos de transmisión entre diferentes puntos.

2.3.1 Controles de acceso al sistema

Los controles de acceso son una herramienta totalmente necesaria y básica para tener un mínimo de seguridad lógica en la entidad. Además son de una gran ayuda ya que protegen a nuestro sistema respecto a modificaciones no consentidas, mantienen la integridad de nuestra información, protegen las aplicaciones que estamos utilizando y protegen la información respecto a empleados que no tienen el acceso necesario para ello.

Cabe destacar que el National Institute of Standards and Technology(NIST) ha compilado los requisitos mínimos que debe de tener cualquier sistema de seguridad:

-Identificación y autentificación del personal.

-Los roles: Consiste en que el acceso a la información por parte del empleado se controla con diversos roles que pueda tener, para cada uno tendrá una serie de privilegios o restricciones dependiendo de cuál sea.

-Modalidad de acceso: consiste en el modo de acceso que puede tener un empleado de la entidad respecto a unos determinados recursos, el usuario puede tener cualquiera de los siguientes modos o todos ellos dependiendo del grado de acceso que tenga:

-Lectura: en este caso solo podrá leer y visionar el documento.
-Escritura: solo podrá modificar dicho documento.
-Borrado: será capaz de eliminar el documento.
-Ejecución: permite el acceso al programa.

-Las transacciones: los controles se pueden desarrollar a través de dichas transacciones, un ejemplo de esto puede ser que para realizar una determinada transacción se solicite una clave determinada.

- Limitando los servicios: este control se centra en las posibles restricciones que pueden existir dependiendo de la aplicación o datos utilizados, todo ello establecido por el administrador del sistema que pone dichas restricciones.

-Horario y Ubicación: en este caso el empleado solo podrá acceder a los recursos en determinadas horas del día y en determinados equipos informáticos de la entidad.

-Control de Acceso Interno: como su nombre indica consiste en un control que se realiza centrado para un posible ataque desde el interior de la entidad, consiste en uso de contraseñas, listas de acceso, cifrado de los datos, etc.

-Control de Acceso Externo: sirve para prevenir un ataque desde el exterior, para ello se utilizan cortafuegos (firewalls), dispositivos de control de puertos, etc.

-Administración: en esta parte consiste en realizar una correcta implementación, pruebas, seguimientos y modificaciones sobre los accesos de los usuarios a los sistemas de la entidad.

2.3.2 Niveles de seguridad informática

Los niveles de seguridad utilizados mundialmente por todas las entidades consisten en la ISO 15408 en referencia a las normas de seguridad en los equipos informáticos del Departamento de Defensa de los Estados Unidos.

Cada nivel tiene una serie de características las cuales describen un nivel de seguridad, estos van desde un nivel mínimo de seguridad hasta el máximo.

Dichos niveles fueron la base para el desarrollo de los estándares internacionales ISO/IEC.

A continuación explicamos todos los niveles.

-Nivel D: Este es el nivel mínimo en el cual solo tiene una división y está guardada para los sistemas que hayan sido evaluados y por supuesto no cumplen con ninguna especificación de seguridad. En este caso no hay autentificación con respecto a los usuarios y por tanto no hay protección referente al acceso de la información.

-Nivel C1 en este nivel se precisa de una identificación por parte de los usuarios para permitir el acceso de información, de la cual no se obtenía en el Nivel D. A partir de ahora se hace la distinción entre los usuarios del sistema y el administrador del sistema, quien tendrá un control de acceso total al sistema. En referencia al nivel C1,

podrán existir grupos de usuarios con iguales privilegios así como grupos de recursos, respecto de los cuales podrá actuar el grupo de usuarios. Por ejemplo: todos los becarios de la uc3m que están trabajando en las aulas informáticas, tienen acceso a una pequeña base de datos que ellos mismos pueden modificar en cualquier momento, por cualquiera de ellos.

-Nivel C2: Este nivel sirve para solucionar las flaquezas que tiene el nivel C1. Consiste en restringir a los usuarios que ejecuten ciertos comandos o que tengan el acceso a ciertos archivos. Los empleados tienen autorización para poder hacer algunas tareas de administrador sin tener que ser administradores. Ayudan a mejorar las cuentas de las tareas centradas con la administración de sistema.

-Nivel B1: El nivel B se divide en 3, este es el primero de ellos, en este caso es capaz de soportar seguridad multinivel, como la secreta y ultra secreta. Se consolida que el dueño del archivo no puede ser capaz de modificar los permisos de un objeto que está bajo el control de acceso obligatorio. El usuario que quiere acceder a un determinado objeto deberá tener un permiso para hacerlo. Consiste en que cada usuario tendrá unos objetos asociados.

-Nivel B2: Consiste en que cada objeto de nivel superior se etiquete por ser padre de un objeto de nivel inferior. En esta parte del sistema, avisará y alertará a los usuarios si sus características de seguridad y acceso han sido modificadas.

-Nivel B3: En este nivel se necesita que la terminal del usuario debe conectarse al sistema a través de una conexión segura. Además aumenta a los dominios con la instalación de hardware. Por último el usuario tiene asignados los objetos y los lugares a los que puede acceder para conectarse.

-Nivel A: es el nivel máximo, para poder llegar a este punto de seguridad, se deben de incluir todos los niveles anteriores. Por supuesto al ser el nivel más alto tiene un proceso de diseño, control y verificación mediante métodos o procesos matemáticos, para garantizar todos los procesos que realiza un usuario sobre el sistema de la entidad. Por último debe de existir protección para que tanto el hardware como el software no tengan infiltraciones ante posibles movimientos del equipo.

2.4 Seguridad física

Respecto a la seguridad física son procesos que existen y sirven para controlar el acceso físico al equipamiento informático. Para ello se usarán cámaras de video, puertas de acceso con tarjetas, etc. Por ejemplo, si visitamos las oficinas de cualquier edificio de una gran empresa veremos cómo tendrán desde la entrada principal del edificio un control para saber quién entra y quién sale, y todo ello automatizado y controlado.

2.4.1 Acceso físico al sistema

Por mucha seguridad que tengamos en nuestro sistema a la hora de acceder a él, no nos sirve de nada si además no somos capaces de tratar la seguridad del acceso físico al sistema, por lo tanto cualquier extraño que entrase en la empresa podría abrir cualquier CPU de nuestra entidad y llevarse físicamente nuestros discos duros con nuestra correspondiente información.

Un caso de ejemplo es el siguiente, el cual está basado en mi propia experiencia, durante estos años de carrera he estado trabajando como becario en las aulas informáticas, y muchos días me he encontrado en la situación en la que una persona totalmente desconocida se ha presentado en el aula, diciendo simplemente ser el técnico de reparaciones sin acreditación ninguna y solo con un destornillador en la mano, esta persona empezó a desmontar las CPU para llevarse supuestamente discos duros, memorias RAM y un sin fin de elementos de una CPU o varias, para supuestamente arreglarlos, quien me dice a mí que en realidad esa persona está robando haciéndose pasar por un técnico, además muchos problemas que había en dicha beca eran los robos de los componentes de las CPU y creo que es un grave problema de seguridad que tiene la UC3M respecto a las aulas informáticas.

Otro caso de ejemplo consistiría en que personas ajenas a la entidad utilicen un disco de arranque con el fin de montar los discos duros de nuestra propia entidad y extraer nuestra información. Para llevarlo a cabo tendría que entrar físicamente a nuestra empresa.

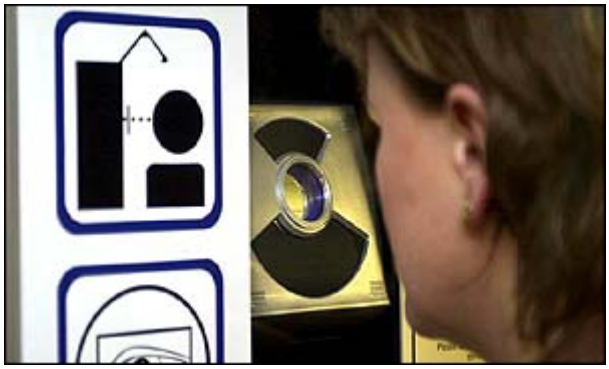
Después de estos casos de ejemplo se debe de garantizar la seguridad física ya que también puede ser un agujero de seguridad de acceso a nuestros datos, por lo tanto para poder prevenir estos casos se recomienda el uso de diferentes sistemas de prevención, cada uno depende de la inversión que se quiere realizar para la seguridad. Estos son los siguientes:

Sistemas de prevención	**Inversión**
Uso de hardware, desde analizadores de retina, uso de videocámaras, uso de control de puertas, personal de seguridad en el edificio, etc.	Alta
Uso de lectores de código, con el fin de saber quién entra y quién sale en cada determinada sala de nuestra entidad con el fin de tener un control sobre su acceso.	Media
Bloquear las tomas de red que no son utilizadas así como los cables de red para evitar pinchazos por terceras personas, cerrar todas las puertas con llave al salir.	Baja

Tipo de inversión ALTA:

Uso de hardware:

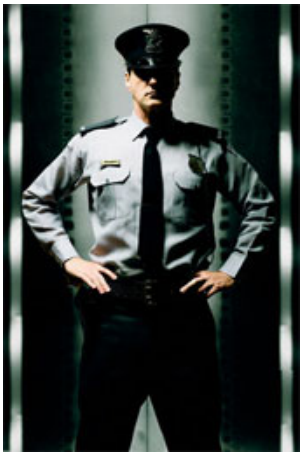
Analizadores de retina:



Videocámaras:

Control de puertas:

Personal de seguridad:



Por último cabe destacar que por mucha prevención que haya nunca es suficiente y por tanto hay que detectar los posibles ataques lo antes posible, para disminuir el daño que vamos a recibir. En este caso hay que concienciar al personal de la entidad, sobre la seguridad del entorno físico, con el fin de que en caso de que se encuentren en el edificio con personal no autorizado se ponga en contacto y avise a la seguridad de la entidad.

Tipo de inversión MEDIA:

Son métodos asequibles por cualquier entidad.

Tipo de inversión BAJA:

Esta inversión es la más barata, debido a que son acciones cotidianas y de sentido común. Aun así también suelen darse problemas.

2.5 Sistemas de seguridad

2.5.1 Autentificación del personal

Esto consiste en la verificación del personal de la empresa, es decir en confirmar que el usuario que va a usar y manejar los datos es el usuario que creemos que es.

Para acceder a un sistema lo más común es utilizar una contraseña o incluso dos para controlar el rango de acceso, aun así existen otras técnicas que hacen lo mismo, y estas se dividen en tres clases dependiendo el tipo de información que se necesita para la autenticación con el fin de obtener el acceso a los datos.

Por lo que se tiene: es decir el uso de una tarjeta electrónica o magnética.

Por lo que se sabe: este es el método más clásico, el uso de contraseña.

Por lo que se es: biometría, es decir el uso de huellas digitales u otros sistemas.

Para un uso mejor recomiendo el uso como mínimo de dos clases, siendo siempre uno de esos dos la clase de "Por lo que es", ya que si solo usamos un método en el caso de que fuera de la clase de "Por lo que se tiene" o "Por lo que se sabe" tiene lagunas de seguridad como el posible robo de contraseñas o robo de la tarjeta electrónica o magnética del empleado, y por tanto creando un serio problema a nuestra seguridad, dejando el acceso a los datos en una situación comprometedora.

Más adelante comentaremos cada una de estas formas, por separado, de control de acceso y de seguridad a los sistemas y datos de la entidad.

¿Para qué sirve identificarse?

La identificación sirve para tener una barrera de seguridad mínima, con el fin de evitar posibles daños a la entidad, además con la identificación podemos entrar en nuestro sistema con nuestras características correspondientes como usuario.

¿Por qué estarían interesados en destruir o robar datos de la entidad?

Podemos responder a esta pregunta en una sola frase, "QUIEN TIENE LA INFORMACION CONTROLARÁ EL MUNDO", si nos fijamos en el mundo que tenemos a nuestro alrededor comprobaríamos que todo se almacena en bases de datos como por ejemplo, cuentas bancarias, historiales clínicos, datos financieros, fichas policiales,

inversiones, Hacienda, etc.; hasta el punto de que por ejemplo un banco si quiere saber todo el dinero que tiene no le sirve de nada contar el dinero físico que tenga en las cajas fuertes, sino el que se indica que tiene en su base de datos. Por lo tanto esa información, que es bastante golosa para terceras personas, tiene que estar a salvo de cualquier posible robo o destrucción de datos, estos son conocidos como delitos informáticos.

¿Quiénes estarían interesados en destruir o robar datos de la entidad?

Pueden ser desde, personas que no tienen ninguna relación, pasando por empleados de la misma compañía o compañías competidoras, las comentaremos a continuación.

Personas sin relación con la entidad, en este caso pueden ser de dos tipos:

Hackers: son personas que atacan a la compañía con el único objetivo de encontrar brechas en el sistema de seguridad y obtener así solo el reconocimiento personal de haber encontrado esa brecha de seguridad en el sistema, son conocidos por el nombre de *"hackers"*.

Crackers: en este segundo caso son personas cuyo objetivo es encontrar esas brechas de seguridad con el fin de obtener los datos de la entidad ya sea para robarlos para su beneficio o destruirlos por puro placer y malicia, se les conoce por el nombre de *"crackers"* los cuales además de utilizar sus habilidades de informática para romper los sistemas de la entidad son capaces de colapsar los servidores, entrar a zonas restringidas de la entidad o compañía para luego infectarlas y apoderándose de ellas.

Empleados de la misma entidad: en esta parte los mismos empleados pueden atacar a su misma empresa por varias razones como por ejemplo: por que están descontentos con la entidad debido al trabajo que desempeñan, al trato que reciben por parte de sus compañeros o sus superiores y el último y por lo tanto el peor de todos los casos es

porque serán despedidos en cuestión de días, su único objetivo será corromper, modificar y destruir datos de la entidad por pura venganza. También es uno de los más peligrosos debido a que ellos tienen acceso a los datos y no se sospecha de ellos.

Compañías competidoras: muchas empresas que compiten en el mismo mercado que nuestra propia entidad pueden llegar a hacer cualquier cosa con tal de eliminarnos de su competencia, ya que nos pueden ver como una seria amenaza para ellos, por ello a veces algunas empresas (no todas), de forma ocasional, pueden ser capaces de atacar, espiar o robar con tal de obtener una gran ventaja respecto a su competencia en el mercado, aunque para ello realice un acto delictivo. Se puede explicar con una frase "En el amor y en la guerra todo vale", y al fin al cabo a la hora de entrar en el mercado de las grandes empresas es una guerra.

2.5.1.1 Por lo que se tiene

Un tipo de seguridad para la identificación del usuario es mediante el control y comprobación de un objeto que tiene la persona y que le identifica como tal usuario y poseedor de dicho objeto, este objeto puede ser una tarjeta magnética o una tarjeta electrónica(smart card). Para la identificación de una persona a través de un objeto se suele utilizar alguna de estas dos clases de tarjeta, aunque últimamente empieza a estar en desuso la tarjeta magnética y está ganando adeptos la tarjeta electrónica (smart card), aun así vamos a identificar a continuación los dos tipos de tarjetas con sus correspondientes características.

2.5.1.1.1 Tarjetas magnéticas

Son una serie de tarjetas que almacenan datos a través de una banda magnética con la cual se pueden grabar datos en ella. Consiste simplemente en una tarjeta de plástico a la cual se le añade una banda magnética en el proceso de su fabricación.

La banda magnética consiste en una banda oscura, la cual está formada por partículas ferro magnéticas insertadas en una matriz de resina y que son capaces de almacenar información a través de una codificación determinada que es capaz de polarizar dichas partículas.

Dicha banda magnética es leída o grabada a través del contacto físico introduciéndola a través de una cabeza de escritura/lectura mediante la inducción magnética. Se

introduce en el lector de tarjetas el cual suele ser como el de la figura de a continuación.

Sus principales características son:

-De bajo costo para la entidad

-No son reutilizables, es decir si la tarjeta ha terminado de hacer su función no puede ser utilizada para otra diferente, a menos que vuelvan a ser grabada en ella nuevos datos.

-Pueden ser leídas y grabadas todas las veces que se desea.

-Aunque son capaces de almacenar información su capacidad es baja.

2.5.1.1.2 Tarjetas electrónicas (smart card)

Consisten en ser una tarjeta de plástico igualmente que las tarjetas magnéticas con la diferencia de que se ha quitado la banda magnética y ha sido sustituida por un chip que consiste en un microprocesador. Estas tarjetas son la evolución de las tarjetas magnéticas, estas tarjetas electrónicas a las cuales al incorporar un microprocesador consiguen tener mayor capacidad de procesamiento que las magnéticas además de ser más versátiles.

Las características de estas tarjetas se centran en lo siguiente:

-Son resistentes al uso continuado.

-Se pueden hacer varias aplicaciones con una misma tarjeta, cosa que no se podía hacer con las tarjetas magnéticas.

-Los datos que contiene están cifrados, además del posible uso de un PIN.

-Tiene una gran capacidad de almacenamiento.

-Pueden ser reprogramadas.

Tal como hemos comentado al principio de esta parte, el uso de este tipo de tarjetas sirve para los mecanismos de control de seguridad y acceso.

2.5.1.2 Por lo que se sabe

2.5.1.2.1 Contraseñas

Las contraseñas sirven para verificar que el usuario que esta accediendo al sistema es dicho usuario y no terceras personas, ya que entonces estamos teniendo una grave brecha en nuestra seguridad, para ello se realiza un proceso de verificación de la identidad del usuario en el cual se comprueba que es quien dice ser. Aun así no existe una seguridad total, y por tanto comentaremos más adelante consejos necesarios para reducir esa posible brecha en nuestra seguridad.

Además el uso de contraseñas sería para la entidad un pequeño costo, ya que es lo más barato y mínimo respecto a la seguridad.

En este caso hay un pequeño problema con el usuario y consiste en que si el usuario tiene que recordar varias contraseñas y éste no sea capaz de recordarlas pueda ocurrir alguna de estas dos cosas:

-Que apunte todas las contraseñas en algún sitio, esto sería un grave error ya que entonces estaría en jaque toda la seguridad de nuestro sistema, y por tanto estaría en peligro nuestra información ya que si alguien encuentra el papel donde están apuntadas las contraseñas producirá una brecha enorme en nuestra seguridad.

-Que al final el usuario decida poner la misma contraseña para todos los accesos que necesita identificarse, en este caso, si alguien es capaz de averiguar su contraseña podría entrar en cualquiera del resto de los sistemas que quiera. Ejemplo: muchos usuarios utilizan la misma contraseña de su email que la que tienen como contraseña en su puesto de trabajo. Esto también es una gran brecha para la seguridad de la entidad.

Para que no ocurran dichos problemas se recomienda mentalizar a los empleados respecto al uso de sus contraseñas.

2.5.1.2.1.1 Consejos a la hora de elegir contraseñas

Para empezar indicaremos un par de consejos totalmente necesarios respecto a las claves que hay que elegir.

-Tienen que tener como mínimo 8 caracteres. Esto es debido a que si se hiciera un ataque intentando escribir todas las contraseñas posibles incluyendo todos los caracteres que tenemos se tardaría un tiempo dependiendo de la longitud de la contraseña. En la imagen de a continuación indicamos el tiempo que se tarda en descubrir una contraseña partiendo del número de caracteres que tiene nuestra contraseña.

LONGITUD DE LA CONTRASEÑA	TIEMPO USANDO TODOS LOS CARACTERES	TIEMPO USANDO SOLO MINUSCULAS
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

-No hay que utilizar una contraseña de acceso a un sitio para usarla en otro. Esto es debido a que mucha gente utiliza la misma contraseña para multitud de accesos provocando un gran riesgo en el caso en que se descubra ya que estará en riesgo el acceso al resto de sitios.

-Nunca usar contraseñas numéricas que tengan relación con el usuario, como puede ser, número de teléfono, fecha de nacimiento o de alguna fecha significativa, número de matrícula del coche, o el número de la lotería que juega siempre, etc.

-Toda contraseña debe de ser alfanumérica, es decir números con letras y además intentar que algunas letras sean mayúsculas y otras minúsculas, además de posibles símbolos.

-Nunca hay que utilizar palabras con significado o de un nombre personal, ya que entonces nos pueden hacer un agujero en la seguridad con un ataque de diccionario.

2.5.1.2.1.2 Como proteger una contraseña

La seguridad respecto a la hora de proteger una contraseña no solo recae en el usuario que la tiene, y muchas veces solo echan la culpa al usuario, sino que además también el administrador tiene parte de culpa. Esto es debido a que si la contraseña del usuario cae en terceras manos no solo se compromete al usuario sino a todo el sistema, en el cual el administrador tiene que estar pendiente de un posible ataque.

A continuación daremos una serie de consejos con el fin de proteger una contraseña tanto para el usuario como para el administrador.

-La contraseña debe de ser modificada cada cierto tiempo, semanalmente, mensualmente, etc.; dependiendo de cada caso, en definitiva la contraseña debe de cambiar con el tiempo.

-Siempre habrá que cambiar todas las contraseñas que estén por defecto en el sistema, suele ocurrir que mucha gente no se preocupa por ellas, pero estas contraseñas son fácilmente de conseguir sin ningún esfuerzo.

-Las contraseñas son de uso individual, por tanto no hay que compartirlas o distribuirlas entre compañeros de la entidad. Consejo para el usuario.

-Nunca hay que escribir la contraseña en algún sitio, debe de estar memorizada, ya sea mediante el uso de técnicas nemotécnicas, ya que cualquier persona puede encontrar donde se haya escrito la contraseña poniendo en grave situación la seguridad del sistema.

-No debe de existir una cuenta sin contraseña, esto es un grave error, y por tanto para que esto no ocurra el administrador debe de estar pendiente y repasar que no exista una cuenta sin contraseña.

-Hay que tener cuidado a la hora de introducir la contraseña ya que hay que evitar que nadie vea lo que estamos escribiendo con el teclado.

-Para finalizar nunca hay que pronunciar dicha contraseña en cualquier conversación que tengamos.

2.5.1.2.1.3 Medidas de gestión y protección de las contraseñas

Además de la seguridad que debe de tener el usuario y el administrador también se puede aplicar a la gestión de dicha contraseña a la hora de introducirla en nuestro sistema, teniendo ésta unos requisitos de seguridad, éstos pueden ser:

-Exigencia de una contraseña con una longitud mínima de 8 caracteres, en caso de que sea inferior, no permitirlo como contraseña.

-El sistema no permitirá contraseñas que no sean alfanuméricas, en caso de de que no se cumpla, no permitirlo como contraseña.

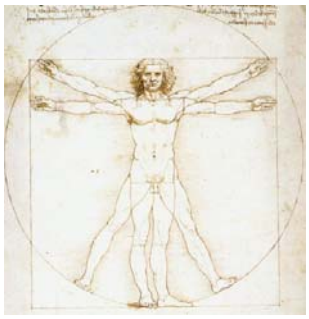
-Tener un número limitado de intentos a la hora de introducir la contraseña, en caso de sobrepasar ese número, se puede bloquear al usuario mientras se envía un mensaje al administrador indicando la situación ante un posible ataque y tomar medidas en el caso más grave.

-Hacer un ataque a nuestro propio sistema con el fin de saber si son vulnerables las contraseñas.

-Indicar al usuario que la contraseña tiene un tiempo de vida limitado y en el caso de que falte poco tiempo para que expire avisar al usuario sobre el cambio de contraseña.

2.5.1.3 Por lo que es (Biometría)

Esta técnica consiste en la verificación del personal de la empresa mediante sus características físicas (voz, huellas, retina, mano, cara, firma, etc.). Esta técnica es una de las más seguras que hay, aun así siempre hay que decir que no existe la seguridad perfecta sin embargo con esta técnica aumentamos bastante nuestra propia seguridad.



Además la biometría tiene una serie de ventajas con respecto a otros sistemas de seguridad, a la hora de la autentificación como por ejemplo:

-No es necesario memorizar ninguna contraseña.

-No es necesario llevar un objeto identificándonos quien es el usuario, a menos que se esté utilizando como método de biometría el "método de 1 a 1", el cual será comentado más adelante.

-No hay que actualizar los registros de los usuarios, la gente mantendrá los mismos rasgos físicos siempre.

-Difícilmente de falsificar dichos rasgos físicos.

El funcionamiento de este sistema consiste en lo siguiente, para empezar el individuo o personal de la entidad se debe registrar en el sistema, obteniendo este último las características físicas de la persona a través de un algoritmo numérico, obteniendo una serie de valores, los cuales se almacenarán en una base de datos.

Ahora cuando el empleado vaya a identificarse existen dos tipos de autentificación el método de 1 a 1 y el método de 1 a N, los cuales comentaremos a continuación:

-Método de 1 a 1, en este caso el usuario deberá identificarse primero a través de una credencial, con ello la base de datos sabrá con que registro deberá comparar los datos que obtenga a continuación de dicho usuario cuando éste se haga la prueba

biométrica, por tanto en este caso los datos obtenidos por el usuario en la identificación biométrica solo se compararán con un registro guardado en la base de datos.

-Método de 1 a N, en este tipo de autentificación el usuario no necesita el uso de ningún tipo de credencial, simplemente se toman los valores del usuario por el sistema biométrico y son comparados con todos los registros que haya en la base de datos del sistema.

Hay varios tipos de clases de biometría según lo que queramos verificar del personal, cada una de ellas tiene sus propias ventajas y desventajas, las cuales comentaremos un poco por encima y que señalaremos a continuación.

Técnica:

Lectura de la mano del empleado:

Ventajas: Poca necesidad de memoria de almacenamiento de los patrones.

Desventaja: Lento y no es muy seguro.

Lectura de la huella digital del empleado:

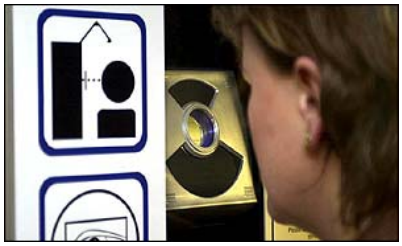
Ventajas: Barato y muy seguro.

Desventaja: Cortes o arañazos que puede tener el usuario pueden ocasionar que no sea reconocido como tal, además existe la posibilidad de una posible imitación.

Lectura del iris del empleado:

Ventajas: Muy seguro.

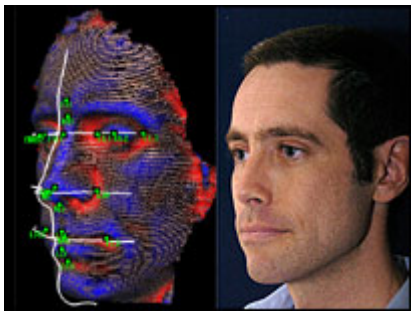
Desventajas: Puede provocar molestias al usuario, o hacer daño a la retina, aunque eso ya no suele ocurrir.



Lectura de la cara del empleado:

Ventajas: Rápido, fácil y barato.

Desventajas: Factores externo como la iluminación de la sala puede alterar dicho reconocimiento.



Reconocimiento de la voz del empleado:

Ventajas: Útil para accesos remotos y baratos.

Desventajas: Si la persona está alterada debido a situaciones emocionales puede no ser reconocida por el sistema.

Reconocimiento de la firma:

Ventajas: Barato.

Desventaja: Puede ser imitado por terceros.

2.6 Criptografía

La criptografía es un punto en la seguridad informática que siempre habrá que comentar, ya que forma parte de ello.

También hay que indicar un error que existe en este mundo a la hora de hablar en relación a este tema y que reside en usar la palabra “encriptar” como si fuese un sinónimo de la palabra “cifrar”.

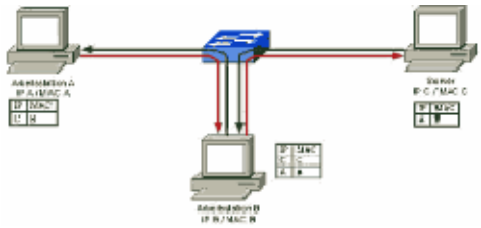
A lo largo del tiempo el ser humano ha intentado ocultar información con el fin de mantener una seguridad mínima para evitar posibles abusos por parte de terceras personas, para ello utilizaba diferentes técnicas de cifrado como por ejemplo el cifrado César o el método de cifrado de Playfair, cifrado Vigenére, etc.

Un ejemplo actual del uso de la criptografía en el mundo de la seguridad informática consiste en los diferentes tipos de cifrado, con el fin de mantener la seguridad de nuestras claves cuando estamos introduciendo una contraseña para acceder a nuestra cuenta de correo o cuando enviamos un correo electrónico para alguien, estos métodos de seguridad sirven para que en caso de que terceras personas sean capaces de obtener dicha información, mediante diferentes métodos de ataque como por ejemplo “el hombre en medio”, no sean capaces de leerlas debido a que están cifradas y por lo tanto no puedan ser leídas por dichos atacantes.

Estas técnicas de cifrado con el paso del tiempo son más complejas para que garanticen una mayor seguridad a nuestra información y sean más difíciles de romper.

A continuación comentaremos un tipo de ataque en el cual para evitarlo habrá que usar medidas de algún tipo de cifrado:

Man in the middle: conocido como ataque del hombre en medio, este ataque consiste en que una tercera persona intercepta un mensaje entre dos personas con el fin de leerlo o modificarlo sin que ninguna de estas dos víctimas se enteren. Para evitarlo se aplican técnicas de autentificación como uso de claves públicas.



A continuación comentaremos por encima diferentes tipos de algoritmos que son usados para cifrar información y poder salvaguardarla en caso de posibles ataques:

Data Encryption Standard (DES): algoritmo de cifrado en bloques simétrico, cuyo tamaño de bloque tiene una longitud fija de 64 bits, y uso de una clave de 56 bits, dicho cifrado se realiza con 16 ciclos de reiteración. Aunque este sistema está en desuso.

Triple Data Encryption Standard (TDES o 3DES): consiste en una variación del DES, y reside en que como su propio nombre indica aplicar tres veces el DES. Dicho sistema usa una clave de 168 bits.

Advanced Encryption Standard (AES): algoritmo más usado en relación a la criptografía simétrica, consiste en un esquema de cifrado por bloques, el tamaño del bloque de datos y de la clave pueden ser de 128, 192 y 256 bits. Es el más usado actualmente debido a su seguridad y rapidez.

3. AUDITORIA INFORMATICA

3.1 ¿Qué es una auditoría?

Para empezar vamos a indicar una serie de definiciones sobre la auditoría.

"Son una serie de técnicas y de un grupo de procedimientos, cuyo fin es evaluar y controlar un sistema con el objetivo de proteger sus recursos y activos, así como comprobar que las actividades que se realizan de forma eficiente y con la normativa general de cada empresa para obtener la eficacia exigida en el marco de la organización estableciendo planes de acción y recomendaciones."

"Consiste en un examen detallado de la estructura de una empresa, en cuanto a controles y métodos, su forma de operación, sus objetivos y planes, sus equipos físicos y humanos".

" Es una visión sistemática y formal con el fin de determinar hasta que parte una organización cumple sus objetivos establecidos por la empresa, así como para diferenciar los que necesitan mejorarse"

"Es una función cuyo objetivo es apreciar y analizar, con vistas a las acciones correctivas eventuales, el control interno de la organización para cumplir la integridad del patrimonio, la autenticidad de la información así como el mantenimiento de la eficacia de los sistemas de gestión."

La auditoría es en sí una actividad que debe de realizarse mediante el uso de conocimientos académicos, para ello se utilizan una serie de técnicas que nos lleven a la prestación de un servicio con alto nivel de calidad y reconociendo la responsabilidad social, no solo del cliente sino del público en general, que necesite hacer el uso del dictamen del auditor, para la elección de decisiones.

3.2 Etapas de la auditoría general

Estudio General:

Está basado en la estimación general de las características de la empresa, de sus estados financieros y de sus elementos más importantes, de forma que nos sirva para la orientación a la hora de aplicar una serie de técnicas que resulten más convenientes en la auditoría.

El concepto que debe de tener el auditor respecto del negocio del cliente es:

- Las condiciones Económicas y del Sector de la Empresa.

- La estructura de dicha Organización.

- Su estructura Legal y Operaciones.

Las condiciones Económicas y del Sector de la Empresa.

El auditor tendrá un conocimiento básico referente a las condiciones económicas de la empresa, así como las condiciones competitivas que llegan a afectar las operaciones realizadas de un cliente y los cambios que se producen en la tecnología. La noción de las prácticas contables relacionadas en el sector de la industria en la cual el cliente se desenvuelve es de vital importancia.

La estructura de dicha Organización

En una organización de cualquier magnitud, será esencial el uso de un diagrama de la organización con el fin de especificar las tareas y las responsabilidades de los diversos miembros de la misma organización. La estructura de una asociación reparte las tareas entre los diversos empleados, las posiciones y departamentos o grupos. Para poder controlar el trabajo de una organización se adoptará medidas de procedimiento y métodos que nos ayudará a proporcionar evidencias de que aquellas tareas fijadas por las estructura de la asociación se llevan a cabo.

Su estructura Legal y Operaciones.

La auditoría comenzará con el conocimiento de las circunstancias y operaciones de la organización auditada. El auditor deberá de preparar una descripción breve de la naturaleza de aquellas actividades comerciales además de los factores más importantes que afectan a dichas operaciones.

Para ello el auditor deberá de tener un conocimiento referente a las características de funcionamiento, así como de los procedimientos relativos a la administración y de su estructura legal.

Para poder comprender la información obtenida mediante la auditoría, el auditor deberá de saber los negocios del cliente así como todos los factores que pueden llegar a influir en las operaciones

La revisión de los documentos legales de la organización es necesaria para el correcto entendimiento de los registros contables, y de sus estados financieros. Con esta información nos ayudará a ampliar el conocimiento del negocio.

Hay que reconocer que sin esta fase del examen de la auditoría sería una restricción referente al alcance de esta área, en la cual sería una negativa por parte del cliente no permitir al auditor contemplar los libros de actas, lo que conducirá al auditor a la denegación de un dictamen. Ya que la información que se puede obtener de ello no se podrá obtener de otra forma.

Ejecución de la Auditoría

Encontraremos los aspectos siguientes en esta etapa:

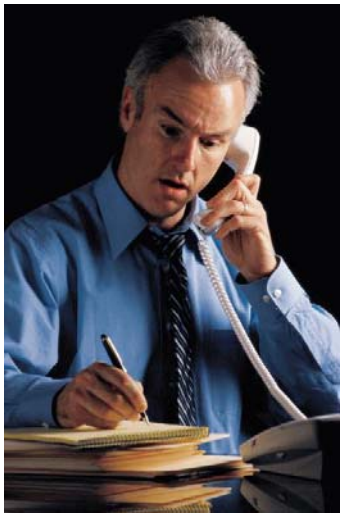
- Análisis: nos ayudarán para clasificar y agrupar elementos de la organización.

- Inspección: se trata de comprobar mediante una serie de pruebas los elementos de la organización.

- Confirmación: consistirá en obtener una comunicación por parte de una persona independiente de la empresa que está siendo auditada para el conocimiento de las condiciones y de la naturaleza de la operación de una manera válida sobre la misma

- Investigación: el auditor obtendrá una serie de conocimientos con los cuales se formará un juicio sobre los elementos de la empresa por medio de datos, ya que estos nos sirven de base para la toma de decisiones.

- Observación: consiste en presenciar los hechos o ciertas operaciones, mediante las cuales el auditor se da cuenta de qué forma se realizan por el personal de dicha empresa.



Informe Final

El informe constará de dos partes la primera será de procedimiento y la segunda una opinión del auditor, con la primera parte se indicará el alcance de dicha auditoría mientras que la segunda será la opinión del autor referente al correcto funcionamiento y presentación de los estados de dicha organización.

El objetivo de este informe será dar una opinión independiente y profesional.

3.3 ¿Cuándo realizar una Auditoría y por qué?

Las razones más importantes a la hora de realizar una auditoría podrán ser algunas de las siguientes.

Razones Externas.

a) Cambio o modificación en el marco legislativo.

- La legislación o la liberación pueden cambiar el entorno, siendo este menos previsible ya que cambia la situación definida por las leyes reguladoras por otra regida por las fuerzas de otras entidades de la competencia.

- La anulación de barreras comerciales obligando a la apertura de nuevos horizontes hacia mercados que pueden tener una competencia internacional en vez de los mercados internos cerrados.

- La privatización de las organizaciones puede cambiar la orientación de ellas mismas, obligando a pasar de un modelo burocrático a un modelo orientado a la eficiencia de las actuaciones y al servicio al cliente.

b) Fluctuaciones del mercado.

- La innovación y la mejora de la tecnología puede llegar a provocar que sectores industriales y las empresas queden obsoletas, para poder solucionar este problema deberán de adaptarse a los nuevos cambios

- Los ciclos económicos pueden llegar a obligar a ciertas organizaciones a cambiar su orientación por lo cual tendrán que tener una serie de estrategias diferentes.

Razones interno-externas

a) La reorganización de una empresa

- Esto puede ser provocado por diferentes causas: ya sea un cambio de la propiedad de la empresa, creación de un producto nuevo, debilitamiento o desgaste en el equipo directivo así como un cambio en la estrategia.

b) Emisión de ofertas públicas en mercados

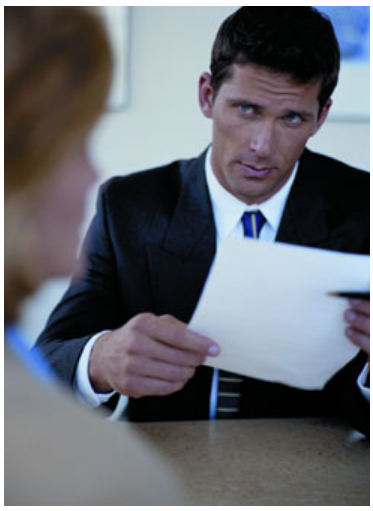
- Debido al éxito de una oferta pública, la publicidad de los resultados obtenidos de la auditoría puede llegar a servir para comunicar las ventajas competitivas de la empresa así como el destacar el talento de los gestores.

3.4 Auditor informático

Para empezar tenemos que saber que un mismo auditor no tiene porqué servir para distintas auditorías, por tanto tenemos que elegir aquella persona que tenga la experiencia necesaria y los conocimientos necesarios acordes al tipo de auditoría que se va a realizar ya que interactuará de una forma más natural.

Su formación académica puede ser desde unos estudios de nivel técnico hasta pasando por ingeniería industrial, derecho, informática, ciencias políticas, contabilidad, o cualquier otra formación, esto es debido a que las auditorías pueden ser de tantas clases como formaciones se tienen, lo importante es que tenga una formación relacionada con la auditoría que vaya a impartir, ya que por ejemplo un auditor en auditoría informática si el día de mañana va a realizar una auditoría fiscal y no tiene los conocimientos necesarios respecto a ese tema, no va a poder realizar el trabajo correctamente aunque su experiencia en auditorías sea alto .

También se valorará toda aquella formación complementaria que habrá obtenido el auditor mediante seminarios, conferencias o cursos de reciclaje.



Respecto a las características personales del auditor las cuales son determinantes a la hora de hacer su trabajo correctamente tiene que tener algunas de las siguientes propuestas a continuación:

-Estabilidad emocional: el auditor no podrá dejarse llevar por sentimientos personales (angustia, rabia, etc.) los cuales pueden influenciar negativamente a la hora de realizar dicha auditoría.

-Escuchar: deberá de estar atento y saber todo lo que está ocurriendo a su alrededor entendiendo claramente lo que digan el personal de la entidad.

-Analizar: tendrá que ser una persona capaz de examinar objetivamente una vez obtenido los datos necesarios.

-Ética: tiene que ser una persona con moral y que no se pueda corromper.

-Observador: tendrá que estar atento a todo lo que está pasando mientras realiza la auditoría.

-Optimista: habrá que dar una actitud positiva a la hora de realizar dicha auditoría para que la gente que esté en dicha entidad no llegue a tomarle miedo, aunque tendrán que demostrar cierto respeto al auditor.

-Objetivo: deberá de tener su propio punto de vista neutral a la hora de realizar el examen final.

-Discreción: su paso a la hora de realizar la auditoría desde la toma de datos hasta la realización del examen debe de pasar lo más inadvertido en la entidad.

-Trabajo en equipo: en el caso de trabajar con ayudantes u otros auditores deberá saber delegar el trabajo, así como una actitud correcta en todo el momento con los demás compañeros del equipo.

-Iniciativa: sabrá qué pasos realizar en cada momento y como tienen que hacerse sin dudar ni flaquear.

-Exposición en público: deberá expresarse correctamente al personal de la entidad.

Por último cabe resaltar que la experiencia del auditor es uno de los mayores puntos a favor que tiene, ya que gracias a ella cada vez tendrá mejores conocimientos y capacidades a la hora de enfrentarse a nuevos retos

3.5 Auditoria informática

Sirve para recoger, agrupar y evaluar evidencias con el fin de confirmar si un sistema de información mantiene la integridad de los datos, salvaguarda el activo empresarial, cumple con los objetivos de la entidad de forma eficiente cumpliendo con las leyes y regulaciones establecidas.

Con esta auditoría podremos mejorar algunos puntos de la empresa como pueden ser la eficacia, seguridad, rentabilidad y eficiencia.

En este tipo de auditoría sus objetivos primarios son, el control de la función informática, el análisis de los sistemas informáticos, que se cumpla la normativa en este ámbito y la revisión eficaz de la gestión de los recursos informáticos.

Pruebas en la auditoría

A lo largo de la auditoría se deben de realizar una serie de pruebas con el fin de obtener la mayor información posible a la hora de tomar decisiones

- Cumplimiento. Sirven para comprobar si un sistema de control interno funciona correctamente.

- Sustantivas. Se obtienen por observación, cálculos, entrevistas, muestreos, técnicas de exámenes analíticos, conciliaciones y revisiones. Sirven para verificar la integridad, exactitud y validez de la información.

- Clásicas. Se comprueban sistemas y aplicaciones con datos de prueba, en un entorno simulado. Observando la entrada y el resultado en la salida obtenido.

¿Cuándo realizar la auditoría?

- Por deficiencias económicas, incrementos de los costes.

- Inseguridad en las instalaciones, ya sea seguridad física, lógica o la confidencialidad de los datos.

- Cuando hay mala imagen o no se cumple con la satisfacción de los clientes, debido a que no se reparan las averían en los plazos que deben de ser, cuando no se atiende correctamente a los clientes, o no se cumplen los plazos de entrega firmados.

- Deben de realizarse cuando se descubren problemas de descoordinación y desorganización, esto es debido a que no se cumplen los estándares de

productividad conseguidos o cuando no coinciden los objetivos o no se cumple con los de la compañía.

Objetivo de la auditoría informática

La operatividad consiste en que la entidad y las máquinas funcionen aunque sea mínimamente. Ya que no es necesario detener los equipos informáticos para descubrir sus fallos y comenzar de nuevo. Este tipo de auditoría se realizará cuando los equipos están operativos, en eso consiste su principal objetivo, que el hecho de realizar la auditoría no pare la productividad de la empresa totalmente. Para conseguir este objetivo habrá que realizar los siguientes controles.

- Controles Técnicos específicos, son necesarios para lograr la operatividad de los sistemas. Por ejemplo se puede descubrir que los parámetros de asignación automática en el espacio de un disco estén mal, provocando que no se pueda utilizar por otra sección distinta. Al igual que la pérdida de información provocando dificultad o anulando otras aplicaciones.

- Controles Técnicos Generales, sirven para comprobar la compatibilidad entre sistema operativo y software, así como la compatibilidad entre hardware y software. Y por tanto es de los más importantes, ya que un problema en la compatibilidad puede crear un gran problema en la entidad.

4.¿QUÉ ES UNA ISO/IEC?

4.1 Introducción

Son estándares de seguridad publicados por la Comisión Electrotécnica Internacional (IEC) y la Organización Internacional para la Estandarización (ISO).

La serie ISO/IEC 27000 sirve para desarrollar, mantener e implementar especificaciones para los sistemas de gestión de la seguridad de la información, también conocido como (SGSI).

Podemos nombrar algunas ISO relacionadas como por ejemplo:

ISO/IEC 27000 – consiste en un vocabulario estándar para el SGSI

ISO/IEC 27001 – es la certificación que deben de tener las organizaciones, además es una norma que especifica los requisitos necesarios para la implantación del SGSI. Se la considera la norma más importante de la familia. Está centrada en la mejora continua de los procesos y de la gestión de riesgos.

ISO/IEC 27002 –Tecnología de la información, técnicas de seguridad y código para la práctica de la seguridad de la gestión de la información.

ISO/IEC 27003 – Directrices para la implementación de un SGSI. También se le considera el soporte de la norma ISO/IEC 27001.

ISO/IEC 27004 - Métricas para la gestión de seguridad de la información. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

ISO/IEC 27005 – Guía para la gestión del riesgo en relación a la seguridad de la información.

ISO/IEC 27006 – En ella se especifican los requisitos para la acreditación de entidades de certificación de sistemas de gestión de seguridad de la información y auditoría.

Cada día son más las entidades que quieren obtener dichas normas consiguiendo así su certificación con el fin de tener un requisito que le permite competir con otras entidades, consiguiendo mayor capacidad de negociación con entidades que piden que sus proveedores y clientes estén certificados.

Otras entidades lo que quieren obtener realmente con dichas normativas es la mejora de sus procesos y acogerse a los estándares de calidad internacionales.

A continuación comentaremos por separado la IEC e ISO, para luego hablar de ISO/IEC.

4.2 IEC

LOGO IEC

4.2.1Historia

IEC surgió en Reino Unido en 1906 y desde sus inicios ha estado proporcionando estándares globales a todas las industrias electrotécnicas mundiales.

La IEC es una organización no gubernamental sin fines de lucro. Su objetivo consiste en publicar y preparar estándares internacionales para todas las tecnologías eléctricas o relacionadas a la electrónica.

4.2.2 Visión

Que las normas de la IEC y los programas de evaluación de la conformidad sean la clave al comercio internacional.

4.2.3 Misión

La misión de IEC es ser reconocida mundialmente como el proveedor líder de normas, los sistemas de evaluación de la conformidad y servicios relacionados necesarios para facilitar el comercio internacional y aumentar el valor del usuario en los campos de la electricidad, electrónica y tecnologías asociadas.

4.2.4 Importancia del mercado

Al promover la adopción de todas y la utilización de las Normas IEC y los servicios a lo ancho del mundo, la gestión IEC hará todo lo posible para garantizar que los miembros de los comités nacionales representan todos los intereses nacionales en tanto el sector privado y el sector público. Estos incluyen a los fabricantes, servicios públicos, proveedores, distribuidores, usuarios, consumidores, investigadores, académicos, normas de las organizaciones de desarrollo y los reguladores.

El IEC seguirá poniendo de relieve el papel esencial de su representante en los comités nacionales, reconociendo tanto que es a través de una buena representación de los comités nacionales y que la industria puede influenciar el trabajo de la IEC y que la mayoría de los costos de la IEC normalización son sufragados por los patrocinadores de expertos que realizan el trabajo técnico.

El IEC hará hincapié en el carácter democrático y transparente de su organización y funcionamiento, que ofrece igualdad de oportunidades a todos los miembros en beneficio de acuerdo con sus contribuciones a la actividad técnica de la IEC.

A fin de maximizar aportaciones y beneficios a sus principales mercados, el IEC desarrollará los medios y procesos mediante los cuales se puede atraer e incrementar sustancialmente la participación de la industria en su normalización y gestión de los organismos de evaluación de conformidad.

Para garantizar la mayor aceptación posible de trabajo IEC y reflexionar sobre la evolución de la sociedad, los comités nacionales de la IEC fomentarán la participación de los usuarios finales y los consumidores a nivel nacional y como los miembros de sus delegaciones.

El IEC se esforzará por aumentar su aceptación como una plataforma mundial para una plena serie de publicaciones técnicas de los documentos de consenso limitado a un consenso pleno las normas internacionales, así como para la evaluación de la conformidad sistemas y servicios relacionados con las normas.

4.2.5 El IEC como una herramienta estratégica.

El IEC debe mejorar su promoción, marketing y comunicación esforzando con los tomadores de decisiones en la industria, gobiernos, reguladores y las organizaciones intergubernamentales sobre los beneficios estratégicos de los productos y servicios de IEC y de participar en su desarrollo y utilización. Entre los reguladores y los países en desarrollo, se prestará especial atención a la importancia de adoptar y en referencia a las normas IEC y de la utilización de sistemas de evaluación de la conformidad de la IEC.

Además, el IEC ampliará su cooperación y comunicación con esfuerzos en los círculos académicos, así como en la industria para desarrollar y proporcionar materiales educativos para el personal técnico y directivos. Estos programas se centrarán en el desarrollo, uso y valor estratégico para negocio de las normas internacionales IEC, los sistemas de evaluación de la conformidad y otros servicios.

El IEC se encargará de dirigir en la evaluación emergentes y convergentes tecnologías y la identificación de nuevas áreas para el desarrollo de normas.

Reconociendo que la industria se centran en torno a la mayoría de la relación costo-efectiva de las estructuras de la normalización que pueda influir o controlar, la IEC seguirá desarrollando mecanismos efectivos, herramientas y procesos innovadores para servir a los mercados en rápido movimiento a través de relaciones con los consorcios y ampliado foros y con funcionarios de desarrollo social relevantes que han alcance global.

Con el fin de satisfacer mejor las necesidades del mercado, el IEC considerará alternativas al modelo de negocio como el establecimiento de una unidad de IEC a sí mismo, separado de la estructura existente para todo el consenso de Normas Internacionales, a desarrollar y publicar los documentos de consenso y la limitada

disposición de otros servicios a los consorcios. Industria se anima a asumir el liderazgo, que participa directamente en la dirección y los niveles técnicos.

4.2.6 Alcance mundial

El IEC seguirá fomentando la participación de las nuevas industrializaciones y economías en transición en la familia IEC. Los países candidatos se identificarán y se facilitará la pertenencia para los que quieran y poder

(a) promover y apoyar la aplicación nacional de la IEC y sustituir progresivamente las normas nacionales divergentes (debido a que estén confusas o no estén de acuerdo);

(b) para formar un comité nacional plenamente representativo electrotécnico,

(c) participar activamente en los trabajos técnicos.

Para lograr su misión de facilitar el comercio internacional, el IEC aplicara su política de importancia a nivel mundial para maximizar la aceptación a nivel mundial y la adopción de las normas IEC armonizado a nivel mundial que satisfagan las necesidades de todos los principales mercados.

A fin de maximizar la armonización mundial de las normas IEC y apoyar sistemas de evaluación de conformidad, el IEC se desarrollará y mejorará las relaciones con las conformidades internacionales de los organismos de evaluación.

Con el fin de racionalizar los gastos para las pequeñas y nuevas industrializaciones de países, y alentar a los nuevos miembros, la IEC examinará a través de una fórmula matemática aprobada por el Consejo y se obtendrá el cálculo de las cuotas de los miembros.

4.2.7 Innovación y valor añadido

El IEC sigue respondiendo a las necesidades del mercado en forma oportuna y rentable, el desarrollo y la mejora de herramientas y servicios para ahorrar tiempo y costo. Esto se devolverá para facilitar las inversiones en proyectos futuros y servicios para el beneficio de los usuarios y los estándares de desarrollo.

En particular, la comisión electoral independiente colaborará con los comités nacionales para proporcionar liderazgo en el desarrollo y suministro de innovadores y eficaces herramientas informáticas necesarias para la normalización de la comunidad entera.

Al tratar de agregar valor para el mercado salvaguardando al mismo tiempo las fuentes de ingresos para el futuro, el IEC en conjunto con los comités nacionales investigará y evaluarán una serie de nuevos servicios de información. El objetivo será facilitar el acceso al mercado de la información electrotécnica relacionada con las normas de múltiples fuentes, en especial los comités nacionales, a través de un único, integrado y interfaz de usuario.

4.2.8 Mejora y sostenimiento

El IEC continuará su prudente gestión financiera, el mantenimiento del saldo de los ingresos por ventas entre el comité nacional y la oficina central para salvaguardar la estabilidad financiera de la pertenencia al tiempo que garantiza los recursos necesarios para las operaciones centrales y las inversiones.

El IEC mejorará aún más la cooperación con ISO en las políticas, procedimientos y procesos. También se identificarán y perseguirán nuevas áreas para la cooperación con la ISO (por ejemplo, servicios de subcontratación o tareas entre la IEC y las secretarías de la ISO), que aumentaría las eficiencias de las secretarías y beneficiaria a las comunidades de las organizaciones en su conjunto, mientras que respetando la integridad de cada organización y el mantenimiento de una eficiente, operación independiente IEC para servir mejor a los mercados de la IEC.

El IEC trabajará en estrecha colaboración con la ISO para desarrollar una política coherente enfoque de los derechos de propiedad intelectual.

El IEC continuamente adaptará sus estructuras y procesos internos, que deseen adquirir la mejor información y recursos de calidad de interesados, en particular la industria, para dar prioridad a los trabajos técnicos y mantener su calidad y a la vez cumplir con los requisitos de mercado para la eficiencia de costes y plazos.

El IEC procurará reforzar los recursos directos de mercado a las Juntas del Sector, la revisión sistemática de los mecanismos de funcionamiento de la Justas del sector y la adaptación de su cobertura de sectores específicos, según sea necesario. El objetivo será aumentar la participación de la industria y la toma de decisiones, especialmente en lo que se refiere a las actividades de IEC con los consorcios y foros, en desarrollo o mejora de procesos para identificar los criterios de mercado para los productos de IEC y los servicios de mejor satisfacer las necesidades del usuario.

El IEC continuará mejorando la calidad y eficiencia del desarrollo de la estructura de sus normas. Alternativa participación de los interesados y el documento de modelos de aprobación, así como las estructuras del comité técnico.

El IEC estudiará los medios por los que podrán seguir para optimizar la estructura, la gobernanza, la gestión y el funcionamiento eficaz de sus sistemas de evaluación de la conformidad para satisfacer las necesidades del mercado, para garantizar recursos de dichos regímenes y para apoyar la labor de normalización en el que se basan.

4.3 ISO

LOGO ISO

4.3.1 Historia

ISO surgió en Ginebra (Suiza), su principal objetivo era "la unificación de los estándares industriales y facilitar la coordinación internacional".

La ISO es una organización no gubernamental que forma un puente entre los sectores privados y públicos. Su objetivo consiste en publicar y desarrollar estándares internacionales al resto del mundo.

Hay que destacar que las siglas ISO, provienen del griego ἴσος (*isos*), 'igual'.

Además la ISO consiste en una red de los institutos de normas nacionales de 160 países (y posiblemente vaya en aumento según pase el tiempo)

Cabe destacar que todas las normas desarrolladas por ISO son siempre voluntarias ya que la ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo que no tiene autoridad y por tanto no puede imponer a un país.

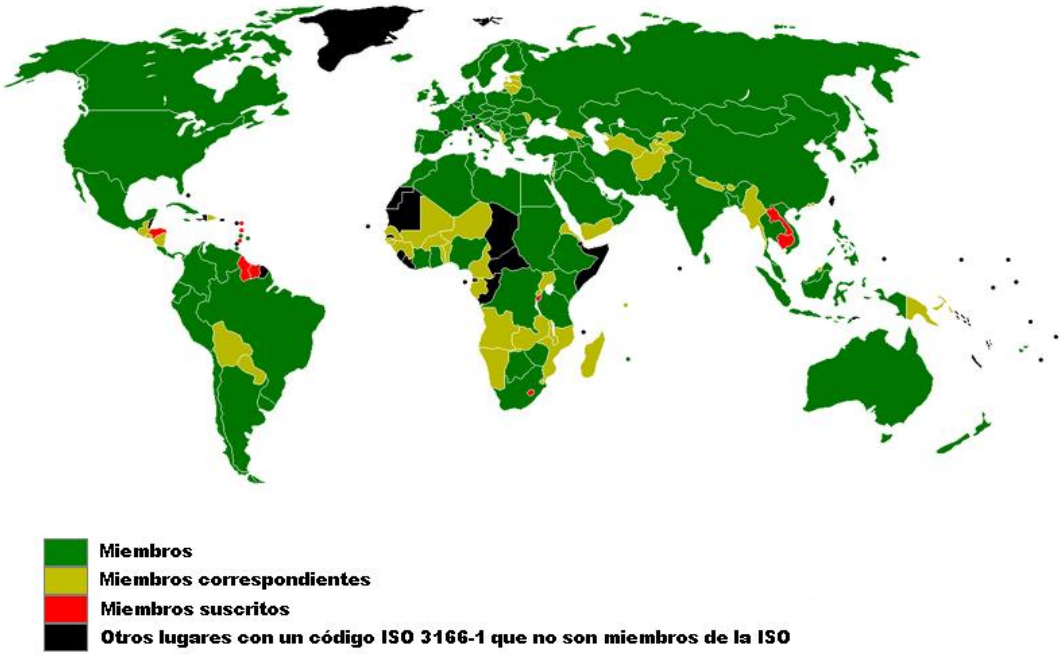
Respecto a su organización se divide en tres clases las cuales son las siguientes:

a) Miembros natos

b) Miembros correspondientes

c) Miembros suscritos

Existe una cuarta clase que simplemente son aquellos los cuales no son miembros de la ISO.



4.3.2 ¿Quién trabaja en ISO?

El trabajo de ISO es muy descentralizado, se lleva a cabo mediante una jerarquía de unos 2850 comités técnicos, trabajos en grupo y otros subcomités. En estos comités los representantes de las industrias, consumidoras, autoridades gubernamentales y organizaciones internacionales de todo el mundo trabajan juntos con el fin de obtener una resolución con todos de acuerdo de los problemas de estandarización a nivel global.

4.3.3 Plan estratégico 2005-2010 de la ISO

4.3.3.1Prólogo

El Plan Estratégico 2005-2010 esboza la visión global de la organización en 2010, junto con los siete objetivos estratégicos establecidos para satisfacer las expectativas de sus miembros y las partes interesadas y los resultados ISO espera alcanzar.

Este plan estratégico identificará las acciones que deben adoptarse o emprender para lograr estos resultados. Se ha elaborado tras una amplia consulta de los interesados, a través de los miembros de ISO, y de las principales organizaciones internacionales con las que colabora la norma ISO.

4.3.3.2 Visión global de la ISO en 2010

La ISO tiene los siguientes puntos a contemplar:

-La facilitación del comercio mundial

-Mejora de la calidad, seguridad, medio ambiente y protección de los consumidores, así como el uso racional de los recursos naturales

-Difusión global de las tecnologías y de las buenas prácticas,

-Contribuir al progreso económico y social.

A través de la red y la colaboración de sus miembros los organismos nacionales, enlaces internacionales, la cooperación regional y las organizaciones asociadas, ISO constituye una plataforma líder para la producción de mercado de referencia a nivel mundial y estándares internacionales. Los mecanismos de ISO, la creación de consenso, la cobertura multi-sectorial y la capacidad de difundir de manera eficiente y promover su gama de productos son reconocidos y que se basa la industria, autoridades públicas, consumidores y otros interesados, lo que ayudará a materializar el objetivo de "una norma, una prueba y un procedimiento de evaluación de la conformidad aceptada por todos". De esta manera, ISO contribuye a una economía mundial más eficiente y sostenible.

4.3.3.3 Objetivos de la ISO para el 2010

La ISO tiene una serie de objetivos los cuales son los siguientes:

-El desarrollo de una colección coherente y multisectorial de las normas internacionales pertinentes a nivel mundial

La industria, autoridades públicas, consumidores y otros interesados reconocidos, apreciarán y confiarán en el valor añadido de la ISO para la producción de normas internacionales y los resultados que apoyan el comercio mundial de productos y servicios, las infraestructuras transfronterizas y las operaciones, así como la difusión de nuevas tecnologías, nuevos métodos de negocio y la buena gestión y prácticas de evaluación de la conformidad.

-Garantizar la participación de los interesados

ISO, a través de sus miembros nacionales, su red de contactos y alianzas, su conjunto coherente de las prestaciones, su facilidad de acceso electrónico y sus iniciativas, promueve el valor de la normalización voluntaria, permite la adecuada participación de partes interesadas y afectadas en sus trabajos y procesos, y por lo tanto se basa el nivel adecuado de consenso para garantizar que sus resultados sean efectivamente utilizados y reconocidos en los mercados mundiales

-La sensibilización y la capacidad de los países en desarrollo

ISO apoya y facilita el desarrollo de acceso a los países a los mercados mundiales, el progreso técnico y el desarrollo sostenible a través de una mayor conciencia y participación en la normalización internacional y actividades relacionadas (por ejemplo, evaluación de la conformidad). ISO promueve su participación activa en su labor. Que miembros de países en desarrollo tengan acceso a herramientas, procesos y programas que les ayuden a desarrollar su capacidad, participar de manera efectiva en el trabajo técnico de ISO y aplicación de estándares internacionales.

-Estar abierto a las asociaciones para el desarrollo eficaz de las normas internacionales

La ISO promueve la cooperación y la integración que pueden ayudar en la prestación oportuna y eficiente el mantenimiento de una colección amplia y coherente de las normas internacionales y otras prestaciones. ISO también está abierto a la colaboración con organizaciones internacionales y otras entidades con alcance global se dedican al desarrollo estándar, cuando ello pueda contribuir a mejorar el desarrollo y la difusión de las normas internacionales.

-Promover el uso de normas voluntarias como alternativa o como un apoyo a los reglamentos técnicos

Las autoridades gubernamentales son conscientes de los beneficios y las modalidades de la referencia a Normas Internacionales ISO en los reglamentos o como una alternativa para la reglamentación. Participan de manera efectiva en su desarrollo, tanto a través de miembros de la ISO y la colaboración de la ISO con las organizaciones intergubernamentales.

-Ser el proveedor reconocido de Normas Internacionales y guías relacionadas con la evaluación de la conformidad.

ISO, en cooperación con la IEC, ofrece una gama completa de normas y guías para la aplicación y el reconocimiento de las buenas prácticas de evaluación de la conformidad, apta para todas las formas de primera, la participación de las partes segunda y tercera y la evaluación, ampliamente utilizado por los proveedores, evaluación de la conformidad operadores y agentes acreditadores y reconocidos por los clientes y autoridades públicas. Se reconoce claramente que la ISO no está directamente implicada en la evaluación de la conformidad con sus estándares, pero supervisa el uso de su marca en materia de evaluación de la conformidad.

-Proporcionar procedimientos eficaces y herramientas para el desarrollo de una serie coherente y completa de las prestaciones

La ISO ofrece un conjunto claro, completo y eficiente de los procedimientos y herramientas para apoyar el desarrollo de una serie coherente y completa de las prestaciones, apreciado, entendido y aplicado efectivamente por los miembros de ISO y los participantes en el trabajo técnico.

4.4 ISO/IEC JTC1

IEC e ISO establecieron un comité técnico conjunto llamado ISO/IEC JTC1 (ISO/IEC Join Technical Committee). Este comité está relacionado con todos los asuntos de tecnología de la información. La mayoría del trabajo de ISO/IEC JTC1 es hecho por subcomités que tratan con un área o campo en particular.

A continuación comentaremos los subcomités que hay en ISO/IEC JTC:

- ISO / IEC JTC 1/SC 02: Conjuntos de caracteres codificados

-ISO / IEC JTC 1/SC 06: Telecomunicaciones e intercambio de información entre sistemas

-ISO / IEC JTC 1/SC 07: El software y la ingeniería de sistemas

-ISO / IEC JTC 1/SC 11: Medios magnéticos flexibles para el intercambio de datos digitales

-ISO / IEC JTC 1/SC 17: Las tarjetas y la identificación personal

-ISO / IEC JTC 1/SC 22: Los lenguajes de programación, sus entornos e interfaces de software del sistema

-ISO / IEC JTC 1/SC 23: los medios de comunicación, la grabación digital para el intercambio y almacenamiento de información

-ISO / IEC JTC 1/SC 24: Gráficos por ordenador, el procesamiento de la imagen y representación de datos ambientales

-ISO / IEC JTC 1/SC 25: La interconexión de los equipos de tecnología de la información

-ISO / IEC JTC 1/SC 27: Técnicas de seguridad de TI

-ISO / IEC JTC 1/SC 28: Equipo de oficina

-ISO / IEC JTC 1/SC 29: Codificación de audio, fotografía, multimedia e información hipermedia - incluye dos grupos de trabajo: WG 11 - Codificación de imágenes en movimiento y audio (Moving Picture Experts Group - MPEG) y GT 1 - Codificación de imágenes fijas (con dos sub-grupos - Joint Photographic Experts Group - JPEG y Conjunto. Los expertos de la imagen con dos niveles en grupo – JBIG)

ISO / IEC JTC 1/SC 31: La identificación automática y captura de datos técnicas

ISO / IEC JTC 1/SC 32: Gestión de datos e intercambio

ISO / IEC JTC 1/SC 34: Descripción de documentos y procesamiento de idiomas - incluye seis grupos de trabajo, por ejemplo, GT 1: Descripción de la Información (SGML, DSDL, etc.), WG 4: Office Open XML y WG 6: Formato OpenDocument

ISO / IEC JTC 1/SC 35: Las interfaces de usuario

ISO / IEC JTC 1/SC 36: Tecnología de la información para el aprendizaje, la educación y la formación - incluye siete grupos de trabajo, por ejemplo, GT 1 - Vocabulario, WG 2 - La tecnología de colaboración.

ISO / IEC JTC 1/SC 37: Biometría

Esta ISO/IEC tiene los siguientes puntos como características principales:

-Adquisición, desarrollo y mantenimiento de los sistemas de información: reside en tomar todas las medidas necesarias para obtener nuevos sistemas, consiguiendo un desarrollo eficiente y mantenimiento de los sistemas.

-Organización en relación a la seguridad de la información: como se debe trabajar en la seguridad de la información en la entidad, tanto de forma interna como externa.

-Gestión de activos: se debe tener un inventario actualizado y completo de los activos, así como su clasificación, quiénes son responsables de los activos, etc.

-Seguridad ambiental y física: residen en tener una infraestructura física y ambiental adecuada a la entidad.

-Gestión de operaciones y comunicaciones: consiste en asegurar la correcta operación de cada uno de los procesos, incluyendo las comunicaciones y operaciones que se dan en la entidad.

-Cumplimiento: se deben de cumplir los requisitos legales, desde el derecho a la confidencialidad de la información, propiedad intelectual, etc.

-Control de acceso: existirán medidas adecuadas para controlar el acceso a información clasificada.

-Políticas de seguridad: debe de haber políticas organizacionales claras y bien definidas las cuales puedan regular el trabajo que se está realizando en el tema de seguridad de la información.

-Gestión de incidentes en la seguridad de la información: la entidad usará registros para identificar las causas y responsables de dichos incidentes, recopilar evidencias con el fin de aprender de ellos y no volver a cometerlos.

-Evaluación de riesgos en la seguridad: deberán identificar, cuantificar y priorizar los riesgos.

-Seguridad en relación a los recursos humanos: se especifican las responsabilidades de los recursos humanos de la entidad.

-Gestión de la continuidad del negocio: se recomienda tener medidas y planes para hacer frente a los incidentes con el fin de que el negocio siga adelante.

La familia incluye estándares internacionales sobre requerimientos, métrica y medición, gestión de riesgos y el lineamiento de implementación del sistema de gestión de seguridad de la información.

Se adoptó el esquema de numeración utilizando las series del número 27000 a continuación

4.5 Puntos débiles de las normas ISO/IEC

Las normas ISO/IEC sirven para aportar beneficios en los sistemas de calidad a las entidades o empresas, aunque estas normas están creadas para aportar valor en el sistema de calidad, no siempre se cumple el objetivo por el cual es aportada en dicha entidad o empresa.

Su punto débil puede tener como origen en diferentes puntos, el más simple y por tanto el que el mayor número de veces ocurre es que no todas las entidades incluyen la norma como un sistema de calidad, ya que en vez de eso, lo que piensan es solo que la ISO/IEC no es más que una certificación necesaria que proporciona a las entidades ventajas competitivas respecto a sus competidoras, por lo que provoca que el objetivo en vez de estar centrado en el mejoramiento de la calidad, sea en la certificación provocando problemas a la hora de incluirla.

Ejemplo: (una tira cómica)

Esta tira cómica ácida, muestra claramente lo que suele ocurrir muchas veces en algunas de las empresas, su principal objetivo no es el mejoramiento de la calidad, sino el del propio certificado que se obtiene, ya que se obtiene una mejora de la imagen de la empresa desde el exterior captada por los clientes.

La ISO o IEC es la nueva moda, todas las empresas desean tener su certificado como sea, aunque para ello les pueda ocasionar terribles perdidas.

Otro de los problemas que tiene consiste en que con dicha norma se inicia el proceso de implementación de dicha norma sin hacer un proceso de sensibilización a todos los actores de la empresa que facilite dicha implementación, ya que bastantes empresas no están en condiciones de iniciar un proceso de certificación en la norma ISO.

4.5.1Repercusiones de sus puntos débiles

Con estos puntos débiles provoca que la norma ISO o IEC deje de ser un gran valor incluido el sistema de mejoramiento de la calidad, para convertirse en un gran problema que llega a afectar el ambiente o el trato organizacional de dicha entidad, lo que provoca una satisfacción negativa por parte del cliente y obteniendo finalmente que dicha empresa pierda dinero, clientes que se van a otros competidores, denuncias, mala imagen, etc.; lo cual al fin al cabo es el principal objetivo de la empresa.

4.5.2 Posibles soluciones

Implementar un sistema hacia la calidad como ISO/IEC , consiste en hacer ”obligatoriamente” (si se quiere llegar a buen puerto) un proceso de sensibilización que involucre a todos los actores de la empresa(incluyendo altos directivos), consistiendo como sensibilización no como un marco conceptual o una fase académica del proceso, sino ser un proceso que facilite y de concienciación hacia el cambio, obteniendo elementos que creen un ambiente positivo y favorable para el nuevo sistema de calidad en la entidad.

Por tanto primero se tendrá que intervenir en la cultura de la empresa con el fin de que cuando se vaya a recibir dicho sistema tenga una visión positiva por parte de todos.

Se recomienda la intervención de una auditoría en dicha entidad, para saber si la entidad que desea implementar las normas ISO, tienen las condiciones necesarias para dicha implementación ya que en caso de que no fuera así, tendrá graves problemas en un futuro cercano o inmediato.

4.6 Preparación para la implementación de las normativas en una entidad

Para la implementación de las normas hay que hacer un análisis del ambiente del trabajo, son muchas las cosas que hay que tener en cuenta antes de dicha implementación.

Todas las entidades por constituidas que se encuentren no están preparadas para implementar una norma, para ello se necesita más que tiempo de experiencia empresarial, tipo de producto, cobertura del mercado, son indispensables unas condiciones básicas de organización, las cuales son las siguientes:

-Un mínimo de procesos definidos.

-Compromiso por parte de todos los actores de la empresa.

-Una cultura organizacional madura.

-El ambiente laboral debe ser agradable, sano y activo.

-Ser conscientes de la necesidad de mejoramiento.

-Tener una buena planificación

-Orientación hacia el trabajo en equipo de forma eficaz.

Dependiendo de la entidad nos podemos encontrar con diferentes clases de cultura o características que tiene dicha entidad. Las cuales vamos a comentar a continuación para poder reconocerlas en caso de una auditoría:

4.6.1 Cultura madura

Está caracterizada por algunos de los siguientes puntos.

Auto-control o disciplina: Cada empleado de la entidad sabe cuál es su responsabilidad y los controles que ejerce.

Mando: en la entidad existen menos líneas de mando y más liderazgo.

Estrategia a largo plazo: existe en la entidad un plan y visión de futuro, los objetivos están bien definidos y se administra más para el futuro.

Compañerismo: existe un gran apoyo y comunicación entre empleados.

Trabajo en equipo: hay una buena integración del trabajo por los diferentes departamentos que existen.

Control del objetivo: debe de existir un sistema que refleje los logros conseguidos a lo largo del trabajo, se deben hacer mediciones con el fin de saber en qué situación nos encontramos.

La empresa o entidad que tiene estas características también es conocida por ser una gerencia moderna. En este caso las normativas como la ISO, ven en ella una gran ventaja con el fin de mejorar sus procesos de calidad.

4.6.2Cultura inmadura

Está caracterizada por algunos de los siguientes puntos.

Gran dependencia: el poder de la empresa está centrado en la gerencia o en un grupo de personas las cuales son los directivos, no aceptan cualquier sugerencia por parte de otras personas de la entidad, y por lo tanto el resto de los empleados realiza lo que se les manda.

No hay suficiente motivación: la única motivación que existe puede ser o por el salario que cobra el empleado o por las amenazas que puede recibir, como puede ser un despido, o el rumor de aplicar un E.R.E. obteniendo así que la gente trabaje bien y que no haya quejas por parte de los trabajadores, también puede ocurrir que simplemente no existe ninguna motivación. Existencia de mobbing.

Perspectiva a corto plazo o no existe estrategia: los problemas que surgen en la empresa se realizan día a día, no se piensa nunca lo que puede ocurrir a largo plazo, provocando que a lo largo surjan mayores gastos para la empresa.

Pasividad del personal: al no existir ninguna motivación, los empleados solo trabajan lo justo por la empresa.

Explotación del trabajador: las empresas abusan del trabajador, como puede ser realizando más horas de trabajo, las cuales no estaban planificadas desde un principio, esto provoca mal estar en el empleado.

Tradición: las empresas se apoyan siempre en frases hechas con el fin de hacer las cosas de la misma manera y no tratar de cambiarlo aunque suponga una mejora en el proceso. Como por ejemplo frases de tipo, “siempre se ha hecho así”, “siempre funciona a nuestra manera”, “para qué cambiar si funciona”.

La empresa o entidad que tiene estas características también es conocida por ser una gerencia tradicional. En este caso las normativas como la ISO/IEC, ven en ella una gran amenaza ya que ven en ella algo que va a tener que modificar el sistema de la empresa y por tanto a producir cambios en ella. Tienen miedo al cambio.

4.7 Diferencias de gerencias(respecto a la cultura inmadura y la madura)

Hay que destacar que la cultura inmadura también es conocida como la tradicional, mientras que la madura es la nueva gerencia también conocida como gerencia moderna la cual se está realizando de una forma correcta con el fin de que la implantación de las normativas cause una mejora en la calidad y no un problema como puede surgir en la cultura inmadura.

Cultura inmadura – Gerencia tradicional	**Cultura madura – Gerencia moderna**
Se centra en aspectos internos rutinarios.	Hace todo lo posible por definir estrategias.
Está orientada a utilidades y además solo a corto plazo.	Fija su objetivo a resultados económicos a largo plazo.
El empleo está asociado a salario económico por eficiencia del personal.	El empleo está asociado a la realización personal.
Estímulo económico por eficiencia	Estímulo por resultados.
Estilo directivo centralizado y autocrático.	Estilo participativo y descentralizado.
Actualiza procesos técnicos y en máquinas	Mejora valores e interviene las actitudes negativas del personal
Énfasis en costos, control de lo existente.	Centrada en innovar y asignar recursos a la generación de valor agregado con el fin de obtener beneficios.

Al fin y al cabo cualquier tipo de entidad, incluyendo la gerencia tradicional, puede implementar las normativas, obteniendo su certificado, pero probablemente no todas van a conseguir una mejora en la calidad de la entidad.

Por lo tanto, ahora tenemos que saber cuáles son las condiciones que necesita una entidad, para que la implementación de normativas ISO/IEC sea favorable.

4.8 Condiciones para la implementación de una normativa llegue a buen puerto

Para conseguir que sea favorable se necesita que la entidad tenga una mente abierta respecto al enfoque hacia el mercado y de un sistema abierto a cualquier tipo de cambio, y todo ello se manifiesta en condiciones como las siguientes:

-Evolución de la empresa, muestra su orientación a clientes, un enfoque hacia el mercadeo integral, creatividad y la disposición al cambio y a la mejora continua.

-Busca la estandarización productiva y más flexibilidad en lo administrativo, para la innovación continua., intenta romper esquemas, se actualiza, es flexible y ágil.

-En vez esperar a que los clientes que vayan a la entidad, es la entidad la que busca a los clientes, mediante el uso de técnicas comerciales.

-En vez de centrarse en costos, se centra en la efectividad y productividad en el mercado.

-Tiene que centrarse en la valoración del mercado a través del cumplimiento de metas y de la satisfacción del cliente, en vez de la valoración de resultados a través de los rendimientos financieros.

En una entidad donde tiene una cultura madura, no existe resistencia al cambio debido a la normativa que se vaya a implementar, tiene una gerencia abierta y los directivos de tal entidad son llamados como líderes y no como jefes. Además la cultura madura tiene bastantes características como las siguientes:

- Existencia de proceso lógico aunque los procesos no están estandarizados.

- Los ejecutivos trabajan en equipo.

- Los planes concretos que tiene la entidad son ejecutados y medidos.

-Todas las ideas que surjan para mejorar la entidad son expresadas libremente y además sirven para la participación del empleado dentro la entidad.

- Se estimula a través de metas y resultados que por un control de tiempo.

- Existe una comunicación correcta de forma horizontal y vertical.

- Aquello que es nuevo para la entidad se le trata como un reto y no como un problema que pueda perjudicar a la empresa.

- Hay reuniones entre directivos y empleados de la entidad.

Para la implantación de las normativas se necesita la existencia de un ambiente correcto, ya que de no ser así la implantación de dicha normativa puede llevar a ocasionar serios problemas para tal entidad.

Por tanto es necesaria y a la vez favorable la existencia de que la cultura de dicha entidad manifieste:

- Que tenga los mejores recursos humanos posibles

- Existencia de una organización centrada hacia el servicio a clientes

- Tener una orientación hacia lo estratégico y una mayor delegación de lo operativo.

- Que siempre esté innovando la entidad en métodos, sistemas de trabajo y en los procesos.

Además la organización de la entidad tiene que estar centrada en la búsqueda de:

-Reducir el tiempo para decidir.

- Ser una organización más horizontal.

-Reducir el costo.

-Mejorar el clima organizacional.

-Disminuir niveles organizacionales.

-Estudiar, conocer y comprender a la competencia.

-Evitar el trabajo individual.

-Uso del Benchmarking.

-Uso de más procesos.

-Búsqueda de la innovación

Si una entidad es capaz de conseguir todo esto, podrá obtener los certificados de dichas normativas, lo cual conseguiría que la entidad tome ventaja respecto a sus competidoras, gracias a las ventajas obtenidas mediante la aplicación de las normativas. Las cuales son:

- Motivación por parte del personal.

- Compromiso por parte de los empleados.

- Reducción de los costos de la entidad.

- Mejoramiento de la productividad.

- Obtención de una mayor rentabilidad.

- Tener una mejora de la posición en el mercado respecto a los competidores.

Cabe destacar que cuando se vaya a hacer la implementación de la normativa hay que vigilar que la entidad no se aleje de centrarse en importantes puntos estratégicos, los cuales durante la implementación pueden ser dados de lado. Como por ejemplo:

-Uso de un sistema participativo.

-Uso del Just-in-time

-La mejora continua.

-La seguridad en la entidad.

-La calidad del trabajo por parte del trabajador.

-La participación de la administración.

4.9 Problemas que surgen en la implantación de la normativa

A la hora de la implementación de la normativa por parte de la entidad pueden surgir bastantes problemas los cuales habrá que evitar y fijarse para que la entidad no caiga en ellos, ya que entonces estamos cayendo en un gravísimo problema.

Se pueden destacar los siguientes problemas:

-Que la entidad se ponga un ritmo de trabajo para la normalización el cual no es el suyo propio (de la entidad y de sus empleados) sino que es en realidad el ritmo del consultor, lo que provoca que no haya una asimilación correcta por parte de la entidad y de sus empleados. Además hay que saber que en este caso no se puede comparar con otras entidades ya que cada entidad está estructurada de forma diferente que el resto y por tanto tendrá su propio ritmo, aun así se pueden establecer unas medias de tiempos para saber entre cuánto van a tardar, pueden ser de entre 11, 12 meses hasta 18, 19, incluso si es necesario un poco más de tiempo, todo esto depende del personal de la empresa.

- No creer que todos los empleados de la entidad están satisfechos tras aplicar la fase de inicio (sensibilización) de la normativa, siempre existen empleados que son más reticentes a la hora de los cambios, por tanto habrá que realizar más esfuerzo en convencerles, ya que entonces si no les hacemos caso nos pueden ocasionar problemas en un futuro inmediato por tanto hay que hacerlo antes de que surjan dichos problemas.

-Que los trabajadores no sean informados de lo que ocurre en la empresa. Esto también es un grave problema ya que les da a entender que no son nadie en la entidad.

-Crear la existencia de un comité de calidad para la entidad el cual solo está formado por los directivos o ejecutivos de la empresa, esto provoca siempre que los empleados de la empresa creen que están conspirando o tramando algo contra el método o los controles que aplican los empleados en su trabajo, esto ocasiona en la mayoría de las veces un mal ambiente de trabajo,

por tanto para poder solucionar este problema tendrá que haber como mínimo un representante de los empleados en dichos comités para que no ocurran estos problemas.

-El consultor el cual sea especialista y sepa cómo aplicar la normativa, no sea capaz de motivar al personal de la entidad, esto que aunque puede no ser muy importante es más trascendental que otras cosas, debido a que el grado de optimismo de los empleados es una baza importantísima para la entidad.

-Transformar el proceso de certificación que se va a implementar en una amenaza para los empleados, este es el mayor problema que puede existir y el primero que hay que evitar, ya que entonces si se toma como una amenaza, lo más seguro que pueda ocurrir es que no sea llevado a cabo.

- Que dicha implantación de la norma se haga por imposición, uso de frases como por ejemplo: “es lo que hay y vamos a hacerlo”, puede provocar el malestar general por tanto se recomienda hacerlo por convencimiento de los empleados, no hay que utilizar nunca el lenguaje soez.

-La implantación se hace simplemente porque está de moda tener dicha normativa con su correspondiente certificado, para dar una imagen que no se tiene en realidad.

-Dar de lado otros programas de la entidad con el fin de obtener dicha certificación, ya que entonces estamos perdiendo calidad en vez de mejorar.

5.¿QUÉ ES UNA METRICA?

5.1 Introducción

Gracias al uso de las métricas estas nos sirven para poder entender el proceso técnico que se está aplicando para crear o desarrollar un producto, ya que a través de ellas somos capaces de medir dicho producto para saber cómo mejorar su calidad.

La medición de los productos es algo totalmente necesario para obtener un producto con gran calidad con el fin de poder entrar en el mercado y competir contra los demás. Sin embargo existe un problema respecto a dicha medición y es que surjan preguntas como las siguientes a la hora de elegir qué tipo de métrica hay que realizar.

Ejemplo:

¿Qué hacer con los datos que obtenemos de dicha métrica?

¿Hay que aplicar la métrica solo con el producto, o también con el resto de la cadena que interviene como son los empleados y procesos?

¿Qué métrica es apropiada para nuestro producto, el empleado y para el proceso?

Estas son un ejemplo de las preguntas que surgen a la hora de buscar y realizar una métrica, sin embargo hay varias razones por las que tenemos que utilizar la métrica con nuestros procesos, empleados y productos. Las razones son:

-Saber la calidad de nuestro producto, con el fin de saber en qué aspectos hay que mejorarlo.

-Conocer si los empleados que están realizando el producto lo están haciendo de forma eficaz y rápida.

-Saber los beneficios de los nuevos procesos, herramientas y métodos que se aplican para obtener el producto.

Todas las métricas que se pueden hacer para medir la calidad del software se agrupan en dos categorías diferentes dependiendo del tipo de métrica que se realice:

a) Métrica indirecta: en esta se centran en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, etc.

b) Métrica directa: respecto a esta se engloba en velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, etc.

5.1.1 Conceptos básicos de métricas

Para empezar a hablar de métrica hay que diferenciarla de otras palabras como medida y medición las cuales son asociadas a la palabra métrica para decir lo mismo cuando en realidad tienen otro significado. Las comentamos a continuación.

Medida "nos proporciona una indicación cuantitativa de cantidad, dimensiones, capacidad, tamaño y extensión de algunos de los atributos de un producto o de su proceso"

Medición: proceso por el cual los números son asignados a atributos o entidades en el mundo real tal como son definidos de acuerdo a las reglas claramente definidas.

Métrica: según el IEEE define la métrica como una medida cuantitativa del grado en que un sistema, componente o proceso posee un atributo dado.

Ahora pondremos frases relacionadas con la métrica por parte de algunos autores

"Cuando puedas medir lo que estás diciendo y expresarlo en números, sabrás algo acerca de eso; pero cuando no puedes medirlo, cuando no puedes expresarlo en números, tus conocimientos serán escasos y no satisfactorios"

Lord Kelvin

"Lo que no sea medible, hazlo medible"

Galileo Galilei

"No se puede controlar lo que no se puede medir"

Tom De Marco

Otras definiciones de la palabra medir según la RAE son:

Medir.

(Del lat. metīri).

1. tr. Comparar una cantidad con su respectiva unidad, con el fin de averiguar cuántas veces la segunda está contenido en la primera.

2. tr. Comprobar la medida de un verso.

3. tr. Comparar algo no material con otra cosa. Medir las fuerzas, el ingenio. U. t. c. prnl.

4. tr. Moderar las palabras o acciones. U. t. c. prnl.

5. intr. Tener determinada dimensión, ser de determinada altura, longitud, superficie, volumen, etc.

Durante mucho tiempo se ha intentado desarrollar una métrica que sea universal con el fin de que sea lo más completa a la hora de aplicarla sobre cualquier producto, por ahora no ha sido posible y han producido, sin embargo, diferentes tipos de métricas las cuales tienen diferentes puntos de vistas.

Gracias a que existen diferentes tipos de métricas, podemos conseguir mejorar la calidad del software ya que con cada una de estas métricas podemos evaluar, clasificar y mejorar el software ya que cada una tiene sus propias características.

5.2 ¿Cómo nos venden la necesidad de aplicar una métrica?

-En el mundo de la industria siempre nos están vendiendo el uso de aplicar la métrica de seguridad, esto es debido al uso del miedo e incertidumbre por parte de algunas compañías para que nos den la sensación de que estamos expuestos a algo terrorífico que puede ser totalmente dañino para nosotros.

-Algunas veces los productos de seguridad se exponen a intrusos con el fin de vendernos que no son posibles de hackearlos y vendernos la idea de una seguridad perfecta y ganar mayor notoriedad.

-Muchos productos que nos venden son sometidos y evaluados por las revistas relacionadas con las industrias mostrando sus principales características.

-Además estos productos están relacionados con las buenas prácticas es decir, lo que se lleva de moda en relación a lo que la industria sugiere como lo más adecuado en dicho momento para nuestra seguridad, como el uso de certificaciones.

5.2.1 ¿Por qué aumentan los ataques a las empresas?

Cada vez con el paso del tiempo el número de ataques se dispara aumentando significativamente y suponiendo un grave peligro para la empresa, esto obliga a que las empresas tengan que estar pendientes de mejorar su seguridad en cada momento con el fin de no encontrarse con una situación de riesgo la cual puede hacer peligrar a la empresa.

Existen varias razones por las cuales estos ataques aumentan y son por algunas de las siguientes razones que exponemos a continuación:

Existe un aumento en la velocidad del desarrollo tecnológico, obteniendo así una mayor curva de aprendizaje y por tanto siempre hay que estar pendiente de actualizarse ya que en cualquier momento se puede quedar obsoleta nuestra seguridad.

El hecho de que no exista el software perfecto hace que los atacantes busquen dicho error por muy escondido que esté y sea este su punto de ataque. No hay nada perfecto, siempre hay errores grandes o pequeños, el objetivo consiste en reducir todo lo posible dicho error por parte de la empresa con el fin de evitar posibles ataques.

La existencia de empleados descontentos en la empresa es otra de las razones por las cuales es una gran motivación para el atacante.

Además los atacantes se aprovechan de la falta de coordinación entre los agentes gubernamentales con el fin de atrapar el delito informático que vayan a cometer. Lo que supone una gran ventaja para los atacantes cuando van a cometer un ataque.

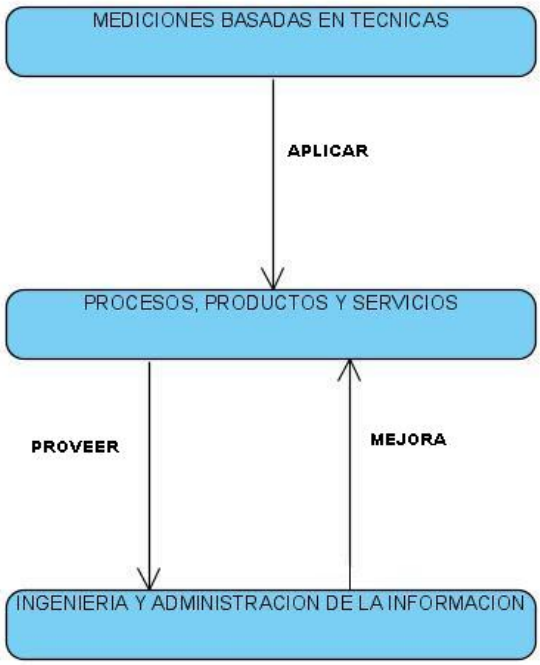
-Con el tiempo las configuraciones de la infraestructura de seguridad se vuelven más complejas con el fin de ser más seguras sin embargo tienen un pequeño punto débil

que consiste en que la probabilidad de realizar una configuración inadecuada aumente y con ello se debilite el seguimiento al control de cambios.

5.3 ¿Qué son las métricas software?

Las métricas software se puede definir como “La aplicación continua de mediciones basadas en técnicas para el proceso de desarrollo del software y sus productos y servicios para suministrar información relevante a tiempo, así el administrador junto con el empleo de estas técnicas mejorará el proceso y sus productos”. Dichas métricas de software proveen la necesaria información para la toma de decisiones técnicas.

En la siguiente figura se muestra un claro ejemplo de la definición puesta anteriormente.



Gracias a las métricas van a ayudar a la hora de evaluar los modelos de diseño y análisis, servirán para mejorar y diseñar nuevas pruebas con mayor efectividad. Mejorando con ello la calidad de nuestro producto.

Para realizar una medición hay que tener unos puntos bastantes claros antes de llevarla a cabo, como son:

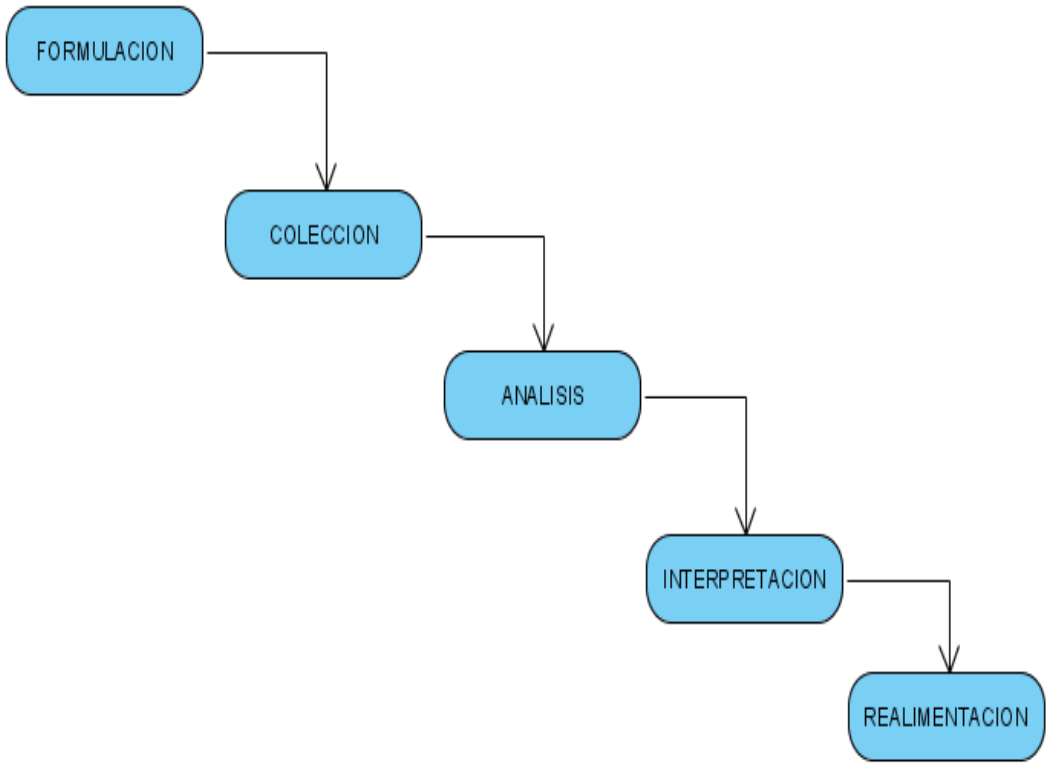
-Las métricas no pueden ser ambiguas.

-Uso de estadísticas

-Automatizar la recogida de datos.

A continuación vamos a indicar un método de un proceso de medición, pero queda aclarar que esto solo es un método de muchos para hacerlo y no es universal.

Para el proceso de medición se recomienda dividirlo en cinco etapas diferentes.



Formulación: en esta primera etapa tiene como principal objetivo el de buscar y elegir las métricas y medidas del software apropiadas para aplicarlo al software en cuestión.

Colección: en esta segunda etapa hay que acumular y obtener todos los datos necesarios y obtenidos del software.

Análisis: ahora con los datos obtenidos en la anterior etapa, se realizan los cálculos de las métricas.

Interpretación: a continuación con los cálculos hechos se realiza su evaluación con el fin de obtener una visión interna de la calidad de la representación.

Realimentación: en esta última etapa se dan las recomendaciones obtenidas de la interpretación de las métricas técnicas trasmitidas al equipo de software.

5.4 Creación de una métrica.

A la hora de crear una métrica debemos de crear una tabla con toda la información correspondiente a dicha métrica, en la cual se indican todas las características que posee que van desde su nombre, propósito, costo que tiene para la empresa, localización, tipo, etc.; todas estas características y el resto de ellas las comentaremos a continuación explicándolas su función.

Titulo:

En este apartado tendrá un nombre significativo para describir la seguridad de dicha métrica.

Propósito:

Se comentará lo que la métrica está diseñada para hacer.

Costo:

Consiste en la estimación de los costes reales de la recogida de la seguridad de dicha métrica.

Tipo:

Definiremos que clase de métrica es, por ejemplo si es técnica o de gestión, si es numérica o textual.

Localización:

Aquí sabremos donde se deben encontrar los datos a recoger, así como los datos previos utilizados con el fin de realizar dicha métrica.

Frecuencia:

Con ello sabremos cuando se deben de recoger los datos así como el número de veces que hay que obtenerlos.

Categoría:

En este apartado deberemos de hacernos una serie de preguntas con las cuales rellenaremos dicho apartado. Las preguntas son:

-¿Cuántas veces sucede algo?

-¿Con qué frecuencia sucede algo?

-¿Cuánto tiempo dura un evento?

- ¿Cuánto cuesta un evento?

Inicio y parada:

Criterios para iniciar y detener la recogida de datos para la métrica de seguridad y para el uso y la presentación de la garantía de dicha métrica.

Duración de la recogida:

Consiste en una estimación o real del periodo en el que se recogerán los datos.

Duración de uso:

Consiste en una estimación o real del periodo en el que se utilizará dicha métrica de seguridad.

Ejemplo de una tabla.

Característica	**Comentarios**
Empleados con entrenamiento complementado	
Propósito	Conocer el tanto por ciento de nuevos empleados que terminaron correctamente su entrenamiento respecto al total de nuevos empleados que entraron en la empresa
Costo	Tiene un costo muy bajo ya que solo hay que revisar el listado de empleados que terminaron correctamente
Tipo	Es una métrica de gestión
Localización	Los datos se tomarán de la sala de recursos humanos ya que son ellos los que llevan el entrenamiento de dichos empleados.
Frecuencia	La frecuencia de dicha métrica es que se realiza cada vez que la empresa contrata a nuevos empleados.
Categoría	Dicha métrica tarda en realizarse unas 3 horas, 1 hora para la recogida de datos y 2 horas para el estudio.
Inicio / parada de criterios	Criterios para iniciar y detener: - Recogida de datos para la seguridad métricas - Uso y la presentación de la garantía de métricas
Duración de la recogida	Los datos se recogerán en una hora respecto al departamento de recursos humanos.

Duración de uso	La duración de esta métrica será de forma continuada, siempre que existan nuevos empleados contratados.

5.4.1 ¿Cómo conseguimos buenas métricas?

Para ello tendremos que usar nuestro sentido común a la hora de interpretar datos de métricas.

Trabajar con equipos y gente profesional para establecer objetivos claros y métricas a utilizar para alcanzarlos.

No utilizar métricas para evaluar a particulares.

En fin, el uso de la medición es esencial para construir el software con calidad.

5.5 Clasificación de métricas

Las métricas se clasifican en diferentes grupos dependiendo de sus características, la clasificación de una métrica de software describe la conducta del software.

A continuación las clasificamos en:

METRICAS EXTERNAS	- Métrica externa de mantenibilidad - Métrica externa de analizabilidad - Métrica externa de cambiabilidad - Métrica externa de estabilidad - Métrica externa de facilidad de prueba - Métrica externa de conformidad
METRICAS INTERNAS	- Métrica interna de desempeño - Métrica interna de complejidad - Métrica interna estilizadas
METRICAS DE CALIDAD	- Métrica de efectividad - Métrica de productividad - Métrica de seguridad

	- Métrica de satisfacción

Ahora las comentaremos una por una, empezaremos por las métricas externas.

5.5.1 Métricas externas

Estas métricas externas están relacionadas con el comportamiento del software cuando está en ejecución.

Métrica externa de mantenibilidad.
En este caso la métrica debe de ser capaz de medir los atributos relacionados como el comportamiento del usuario, personal de mantenimiento o sistema incluyendo el software, cuando dicho software es modificado o se mantiene durante la fase de mantenimiento o de prueba.

Métrica externa de analizabilidad.
Estas métricas son capaces de medir atributos como esfuerzo del personal de mantenimiento, recursos utilizados o del usuario cuando intentan diagnosticar las deficiencias o causas o errores del fallo del software o identificar las partes con el fin de ser modificadas.

Métrica externa de cambiabilidad
Deben de ser capaces de medir atributos como el esfuerzo del personal de mantenimiento, del usuario y del sistema incluyendo el software cuando tratan de implementar una modificación especificada anteriormente con el fin de mejorar un error que se descubrió antes.

Métrica externa de estabilidad
Esta métrica debe de ser capaz de medir los atributos en relación con el comportamiento del sistema cuando tiene un comportamiento inesperado del sistema, incluyendo cuando el software se prueba o se hacen modificaciones con el fin de mejorarlo.

Métricas externa de facilidad de prueba

Debe de ser capaz de medir el esfuerzo del usuario, del personal de mantenimiento y del sistema incluyendo el software cuando están tratando de probar dicho software, además también habrá que probarlo en el caso de que haya sido modificado.

Métrica externa de conformidad
En este último caso, tienen que medir un atributo como el número de funciones y de ocurrencias de problemas de conformidad, que no son capaces de que el producto software cumple los estándares, convenciones o regulaciones relacionadas a la mantenibilidad que se quiere cumplir.

5.5.2 Métricas internas

En esta clase de métricas se miden las características del software en sí mismo, como puede ser el número de llamadas de función o el número de líneas de código que se realizan sobre unos productos software no ejecutable, etc.

Métricas internas de desempeño:
Están relacionadas con las métricas que miden la conducta de sistemas de software y módulos, bajo la supervisión del hardware o sistema operativo. Están relacionadas con la eficiencia de ejecución, almacenamiento, complejidad de algoritmos, tiempo, etc.

Métricas internas de complejidad:
Aquellas cuyas métricas de software que definen la medición de la complejidad, ya sea tomando datos como el tamaño, volumen anidaciones, agregación, costo, flujo y configuración. Estos puntos son críticos para la concepción, análisis, viabilidad y diseño de software.

Métricas internas estilizadas:
Su función consiste en métricas de preferencia y experimentación. Esto significa como puede ser el estilo de código o de programación, limitaciones de datos, etc. No hay que confundir con las métricas interna s de complejidad.

5.5.3 Métricas de calidad

Las métricas de calidad consisten en la calidad en uso, desde el punto de vista del usuario respecto a la calidad del entorno en el cual está presente el software y se mide a partir de los resultados obtenidos de utilizar el software en el entorno. Las métricas de calidad de dividen en cuatro bloques.

Métrica de efectividad

Está relacionada con los objetivos de los usuarios con la completitud y precisión con la que tales objetivos son logrados.

Métrica de productividad

Relacionan el nivel de efectividad conseguido respecto al consumo de recursos utilizados. Algunos recursos relevantes pueden incluir esfuerzo mental y físico, materiales, tiempo y dinero. Uno de los recursos más importantes es el tiempo.

Métrica de seguridad.

Estas evalúan el grado de riesgo de daño que pueden recibir objetos, recursos y personas. Contempla salud y seguridad tanto del usuario como de los afectados por dicho uso, al igual que consecuencias económicas o físicas no intencionadas.

Métrica de satisfacción.

Puntúan la actitud del usuario respecto al uso del producto software y un contexto determinado.

5.6 ¿Por qué? Las métricas de seguridad.

A continuación comentaremos de forma rápida este punto, así como los problemas que encontramos.

¿Por qué se usan métricas de seguridad?

- Gestión de seguridad de la información en una organización.

- Proporcionar información para la gestión de informes.

- Indicar el cumplimiento de la legislación, reglamentación y las normas.

-Apoyo a las actividades de gestión de riesgos.

Principales problemas identificados:

- No hay un propósito claro.

- Dificultad de métricas de seguridad que se refieren a la actividad.

- Incompatibilidad de métricas de seguridad con métricas de negocio.

Lo que se utiliza actualmente y se recoge:

- Incidentes.

- Protección antivirus.

- Gestión de riesgos.

- Revisión de la gestión.

- Cumplimiento de las políticas internas.

- Resultados de la fiscalización.

-Costo.

Principales problemas identificados:

-Difícil para seleccionar parámetros de seguridad.

- Métricas de seguridad orientadas a los negocios.

- Falta de una visión clara, en toda la empresa, de seguridad de la información.

Cómo se usan métricas de seguridad y son presentadas:

-Se otorga a una amplia gama de audiencias.

-Presentado con una variedad de formatos diferentes.

Principales problemas identificados:

- Dificultad para identificar a la audiencia correcta.

- Difícil para seleccionar y combinar el formato de presentación a la audiencia.

Interpretación inadecuada de la seguridad de la información.

5.6.1 Algunas características de las métricas de seguridad

-Tienen que ser fáciles de obtener.

-Expresadas en porcentajes o números en escala.

-Necesarias con el fin de realizar tomas de decisiones.

-Tienen que ser detalladas explicando cada cosa que sea necesario.

5.6.2 Beneficios de las métricas en seguridad.

A través de las métricas somos capaces de obtener bastantes beneficios como por ejemplo:

-Encontrar posibles problemas que surgirán a corto plazo.

-Saber los puntos débiles de nuestra entidad.

-Conocer los riesgos que podemos obtener.

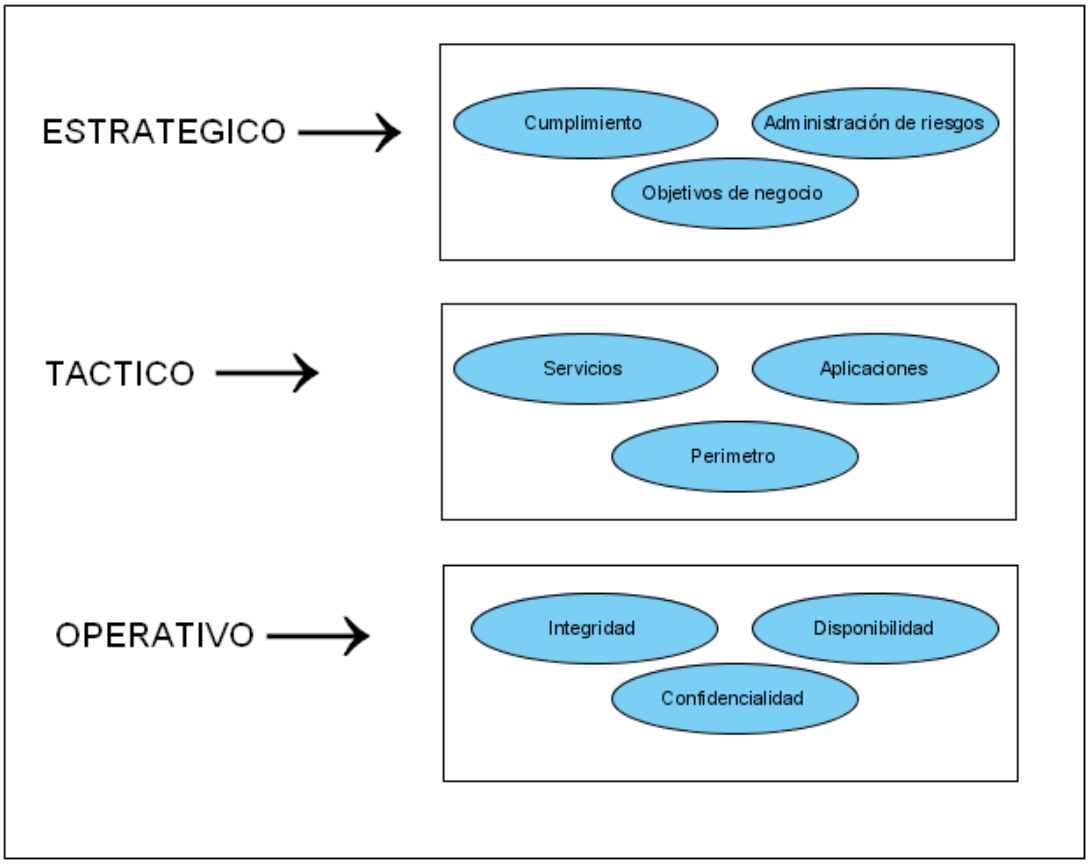
5.7 MEMSI (Modelo estratégico de métricas en seguridad de la información)

El modelo estratégico de las métricas respecto a la seguridad de la información se divide en tres niveles.

a) Nivel estratégico

b) Nivel táctico

c) Nivel operativo.



En el cual cada uno de ellos tiene varios grupos dentro de sí. Los cuales comentaremos a continuación:

a) En el nivel más alto conocido como nivel estratégico encontraremos tres grupos los cuales son:

-Cumplimiento: se centrará en llevar a cabo los estándares de la seguridad informática, realizar auditorías así como las pruebas de cumplimiento.

-Administración de riesgos: la cual consiste en identificación de los activos de la empresa a proteger, realizar ejercicios de análisis de controles y riesgos,

realización de planes de seguimiento y actualización, creación de pruebas respecto a vulnerabilidades así como la creación de mapas de controles y riesgos.

-Objetivos de negocio: este grupo se centrará en las relaciones con los clientes por parte de la empresa, la agilidad y responsabilidad ante incidentes que ocurran, el significado de la seguridad respecto a los procesos de negocio y de las expectativas de la gerencia en relación a la confianza de los sistemas.

b) En el nivel intermedio conocido como nivel táctico encontraremos otros tres grupos los cuales son:

-Servicios: el cual ser encarga del control de cambios, copias de respaldo, posibles recuperaciones ante fallos, el aseguramiento de equipos y la administración de parches.

-Aplicaciones: su responsabilidad es la siguiente, desde revisar el código fuente, defectos identificados en el software, pruebas de vulnerabilidad en software, vulnerabilidades identificadas y utilización de funciones no documentadas.

-Perímetro: este último se encarga de la efectividad de la seguridad que va desde la efectividad del Antispam, antivirus, firewall, así como la efectividad del monitoreo 24*7.

b) En el nivel bajo conocido como nivel operativo encontraremos otros tres grupos los cuales son:

-Integridad: cuya función consiste en eliminar, borrar o manipular datos, como protegerse ante virus informáticos.

-Disponibilidad: se encarga de la negación del servicio, inundación de paquetes, suplantación de datos o IP, eliminar, borrar y manipular datos.

-Confidencialidad: este último debe estar preparado para encargarse desde contraseñas débiles, suplantación de IP o datos, accesos no autorizados por terceras personas, configuración por defecto que puede poner en peligro si no tiene la configuración deseada, monitoreo no autorizado.

5.7.1 Características del modelo

-Se consigue sugerir una manera de integrar los principios de la seguridad informática, los incidentes y las tecnologías de seguridad.

-Exige un diagnóstico y análisis

-Se reconocen las diferentes culturas de dicha organización en diferentes niveles.

-Como parte fundamental para el desarrollo de las métricas se vinculan los objetivos de negocio

-Se reconoce que la seguridad no es un fenómeno no dualista (causa-efecto) sino que es dual (circular)

-Se establece las preguntas que integran dichas expectativas, acciones de los diferentes actores de la organización y los acuerdos.

5.7.2Ejemplos de métricas para la seguridad informática

A continuación comentaremos solo un par de métricas que podemos utilizar para alguno de los tres niveles que hemos comentado anteriormente, queda aclarar que solo son algunos ejemplos y que pueden hacerse muchos más.

Nivel estratégico:

Algunas métricas pueden ser:

-Conocer el % (tanto por ciento) de las cuentas inactivas de usuario deshabilitadas respecto al total de cuentas inactivas.

-Conocer el valor total de los incidentes de seguridad informática respecto al presupuesto total de seguridad informática.

-Conocer el % (tanto por ciento) de los nuevos empleados que completaron su entrenamiento de seguridad respecto al total de los nuevos empleados que entraron.

Propósito de esta métrica: desempeño de personas y procesos.

Nivel táctico:

Algunas métricas pueden ser:

-Conocer el número de mensajes salientes con spyware o virus.

-Numero de mensajes de spam detectado respecto al número total de mensajes ignorados.

-Número de estaciones de trabajo en funcionamiento configuradas correctamente respecto total de las estaciones de trabajo.

-Numero de spyware o virus detectados en estaciones de trabajo o servidores.

Propósito de estas métricas: desempeño de las tecnologías de seguridad informática.

Nivel operativo:

Algunas métricas pueden ser:

-Número de incidentes asociados con la disponibilidad respecto al total de incidentes.

-Número de incidentes asociados con la confidencialidad respecto al total de incidentes.

Propósito de estas métricas: desempeño de la administración de incidentes

6. ISO/IEC 27004

6.1INTRODUCIÓN

El nombre de la normativa es ISO/IEC 27004 Information technology – Security techniques – Information security management – Measurement, cuya traducción en español sería ISO / IEC 27004 Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información – Medida, por lo tanto como su propio nombre indica tocaremos todos esos campos en dicha normativa.

La norma 27004 se creó para complementar a la norma ISO 27001, ya que la norma 27001 destaca que los controles tienen que ser medibles, ya que si no somos capaces de medir un control no nos servirá de nada para nuestro SGSI, por lo tanto hay que hacerlo medible, y es por esa razón por la que se realiza la normativa 27004 en la cual nos enseña cómo debemos medir dichos controles, su objetivo consiste en hacerlos medibles.

Esta normativa 27004 nos sirve de ayuda para guiarnos sobre la creación y el uso de las mediciones con el fin de poder evaluar la eficiencia del sistema de gestión de la información aplicada a los controles y seguridad. Con esta normativa se incluye la gestión de información de seguridad de riesgos, procesos, política, objetivos de control, procedimientos, ayudar al proceso de su revisión, así como ayudar a determinar si alguno de los procesos de SGSI o controles necesitan ser mejorados o modificados.

El uso de esta normativa constituye una medición de la seguridad de la información. El sistema de gestión de la seguridad de la información nos ayudará evaluar y a identificar aquellos procesos o normas ineficaces en nuestro sistema de la seguridad de la información, así como los controles y prioridades de las acciones asociadas.

Gracias a esta norma será un punto de partida para el desarrollo de la medida de medición es importante para la comprensión de los riesgos de seguridad de información donde la entidad o la organización se puede enfrentar o tener problemas. Así como saber que las actividades que está realizando la empresa respecto a la evaluación de riesgos se está haciendo correctamente.

Queda aclarar que el objetivo de dicha normativa consiste en fortalecer la organización y que gracias a la normativa proporciona una información fiable a la entidad sobre los

riesgos que corre en relación a la seguridad de información así como el estado de nuestro SGSI aplicado para la gestión de estos riesgos.

Los datos obtenidos de las mediciones realizadas nos servirán para hacer una pequeña comparación de los avances o progresos obtenidos en referencia a la seguridad de la información en un período de tiempo, comprobando así la mejora continua de la organización en su SGSI.

Esta normativa se puede aplicar a cualquier tipo de tamaño de la organización desde multinacionales repartidas por todo el mundo hasta las PYME, la única diferencia consistirá en la complejidad que tomaría para las multinacionales a la hora de aplicarlo ya que tendría que realizar múltiples programas de seguridad de la información de medición, mientras que en las PYME, las cuales son las medianas y pequeñas empresas, una información menos completa será suficiente. Ya que con una sola medición de seguridad de la información puede ser suficiente para dichas empresas

Además hay que recordad que esta normativa no es obligatoria y no es necesario su uso, como el resto de las normativas ISO/IEC sirven para aconsejar. En este caso esta normativa aconseja sobre las siguientes actividades.

-Medida de desarrollo

-Aplicación y operación de un programa de seguridad de la información en relación a la medición.

-Recogida y análisis de datos

-Elaboración de los resultados de la medición

-Comunicar los resultados de la medición desarrollados para las partes interesadas.

-Utilizar los resultados de medición a la hora de tomar las decisiones relacionadas con el SGSI

-Utilizar los resultados de medición para mejorar el SGSI (alcance, políticas, controles, procesos, objetivos y procedimientos)

-Facilitar la mejora continua de la seguridad de la información

Para finalizar hay que indicar que con dicha normativa nunca se podrá garantizar la seguridad total.

6.2¿El por qué de la ISO 27001?

Gracias a la ISO/IEC 27001 se añade un nuevo concepto de indicador sobre la eficacia de los controles, lo cual provoca que el SGSI (Sistema de Gestión de Seguridad de la Información) sea capaz de evaluar su calidad y su eficacia el mismo.

La ISO/IEC 27001 desea que la entidad u organización tenga que hacer revisiones periódicas de la eficacia de su SGSI en referencia a los resultados obtenidos de la medición de su eficacia, y con esos resultados obtenidos verificar que los requisitos de seguridad se cumplen.

Además también quiere que dicha entidad sea capaz de definir la manera de medir la eficacia de los controles seleccionados o grupos de controles y especificar cómo estas medidas se van a utilizar para evaluar la eficacia de control para producir resultados comparables y reproducibles.

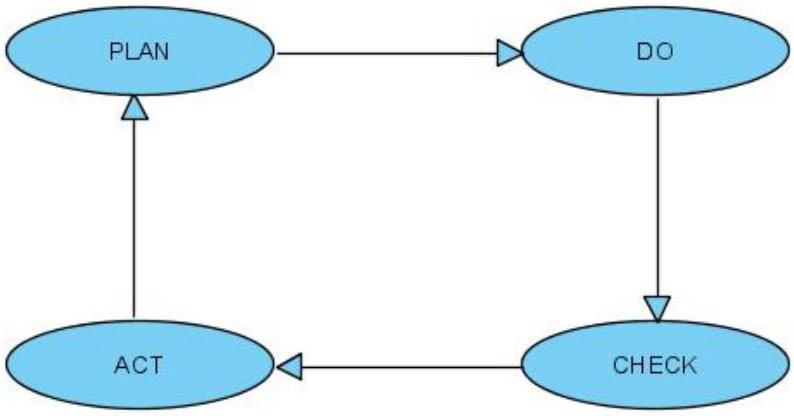
Para la entidad que quiere cumplir los requisitos de medición indicados en la normativa ISO/IEC 27001 varían en relación a la entidad, como puede ser, el tamaño de la entidad, los riesgos que tienen, recursos de la organización, etc. Aun así la entidad tiene que tener cuidado a la hora de aplicar sus recursos y saber repartirlos cuidadosamente para las acciones del SGSI, ya que no debe de utilizar todos los recursos porque entonces dejarían de ser beneficiosos y sería perjudicial debido a que no tendría recursos suficientes para las otras actividades que debe de realizar la entidad. Por lo tanto tiene que tener una buena organización y por tanto aquellas actividades que estén en curso de medición deberían ser integradas en las operaciones regulares de la entidad con un mínimo de necesidades de recursos.

El utilizar métricas de seguridad en el Sistema de Gestión de Seguridad de la Información puede provocar que la norma perdure en el tiempo como un estándar potente y eficaz para gestionar las seguridad de la información de una forma óptima, debido a que las métricas de seguridad no están contempladas como un accesorio más a añadir al Sistema de Gestión de Seguridad de la Información según le interese a la entidad sino que lo absorbe y termina formando parte de él a lo largo de su ciclo de vida. Todo esto provoca que el sistema de medición junto a su Sistema de Gestión de Seguridad de la Información sea revisado y mejorado de una forma continua.

Por ello la ISO/IEC surge a partir de la ISO/IEC 27001.

6.3Las mediciones

La normativa ISO/IEC 27004 está centrada sobre el modelo Plan-Do-Check-Act, también conocido como PDCA, el cual consiste en ser un ciclo continuo y que comentaremos más extensamente en el siguiente punto.



En una entidad se deberá de saber cómo interactúan y se interrelacionan las mediciones de la entidad con su Sistema de Gestión de Seguridad de la Información.

Para ello la entidad tendrá que crear una serie de guías las cuales especifiquen, señalen, documenten y expliquen estas relaciones con el máximo detalle posible con el fin de llevarlo a cabo lo mejor posible.

En los procesos de mediciones se tienen que cumplir una serie de objetivos los cuales son los siguientes.

- Indicar y avisar los valores de seguridad de la entidad.

- Realizar una evaluación de la eficiencia del Sistema de Gestión de Seguridad de la Información.

- Incluir niveles de seguridad que sirvan de guía para las revisiones del Sistema de Gestión de Seguridad de la Información, lo cual provocará nuevas entradas para auditar y para ayudar a mejorar la seguridad de la entidad.

- Realizar una evaluación de la efectividad de la implementación de los controles de la seguridad de la entidad.

6.4Modelo de las mediciones

Para llevarlo a cabo se necesita crear un programa con el fin de realizar la medición de la seguridad de la información de la entidad. El programa deberá centrarse en las ayudas que aportan dichas mediciones a la hora de tomar decisiones.

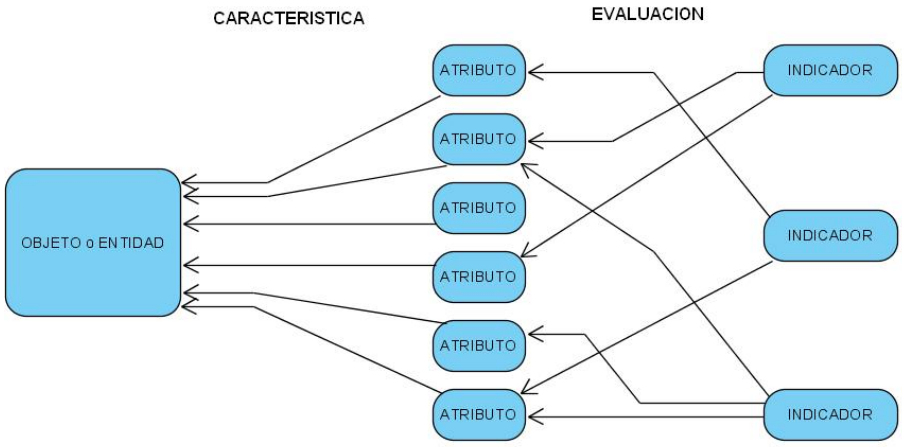
Esto obliga a que dicho programa de medición deba de estar basado en un modelo de mediciones para la seguridad de la información.

El modelo se centra en una arquitectura que relaciona los atributos medibles con una entidad relevante. Dichas entidades pueden incluir, productos, recursos, proyectos y procesos.

Este modelo servirá para describir como dichos atributos son cuantificados y transformados en indicadores que servirán para la entidad a la hora de tomar decisiones.

Para desarrollar este modelo es necesario definir los atributos que son considerandos más importantes para medir la información que la organización necesita.

También se puede considerar que un mismo atributo puede incorporarse en múltiples mediciones para las cuales se tendrán informaciones distintas.



PROGRAMA → MODELO→ ENLAZA (Objetos con atributos)

EL MODELO DESCRIBE COMO SON CUANTIFICADOS

6.5Método de las mediciones

¿Cómo tienen que ser medidos los atributos?

Con esta normativa nos indica cómo los atributos tienen que ser medidos, por lo cual propone un Método.

Existen dos tipos de métodos a la hora de cuantificar los atributos necesarios.

- Objetivos: los cuales se centran en una regla numérica (por ejemplo de 1 a 5) que se pueden aplicar a las personas o a los procesos, se recomienda que se realice primero a los procesos.

- Subjetivos: se centran en el criterio de los empleados o de los evaluadores externos.

Dichos métodos pueden englobar diferentes tipos de actividades y a su vez un método engloba a varios atributos.

Algunos métodos que se utilizan en la entidad con el fin de medir los atributos son:

- Cuestionarios al personal de la entidad.

- Inspecciones de las aéreas de dicha organización.

- Toma de notas a partir de observaciones.

- Comparación de atributos en diferentes momentos.

- Muestreo.

- Consultas de los sistemas.

Una vez realizados los métodos de medición es asociarlo a un tipo de escala, las clases de escala pueden ser:

- Ratio: uso de escalas de distancias.

- Nominal: uso de valores categóricos

- Intervalos: uso de máximos y mínimos.

- Ordinal: uso de valores ordenados.

Para finalizar se tiene que considerar la frecuencia de cada medición. Se recomienda que la entidad programe dicha frecuencia de las mediciones, ya sean diarios, semanales, mensuales, semestrales, trimestrales, cuatrimestrales o anuales.

6.6Selección y definición de las mediciones.

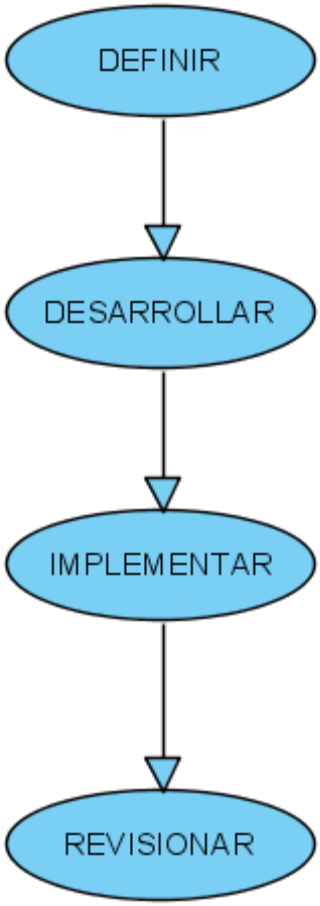
También se indica cómo desarrollar dichas mediciones para cuantificar la eficiencia de nuestro Sistema de Gestión de Seguridad de la Información, controles y procesos.

Dichas mediciones de la información son requeridas para:

- La certificación de nuestro Sistema de Gestión de Seguridad de la Información de la entidad.
- La mejora en la eficiencia del Sistema de Gestión de Seguridad de la Información.
- Para los clientes de la entidad, accionistas, etc.
- Para cumplir con las regulaciones y requisitos legales.
- Para la mejora de los procesos.
- Para la alta dirección de la entidad.

Ahora para poder realizar el establecimiento y la operación de un programa de mediciones necesita realizar los siguientes puntos en orden.

- Definir los procesos
- Desarrollo de mediciones
- Implementación del programa
- Revisión de mediciones.



Las mediciones pueden estar relacionadas con:

- Ejecución de controles de seguridad de la información, como puede ser por ejemplo el volumen de incidencias por tipo.
- Procesos de sistemas de gestión, como puede ser por ejemplo si se realizan las auditorías indicadas.

Además las mediciones tienen que cumplir con una serie de criterios para que sean validadas por la entidad. Los cuales son:

- Cuantitativo: uso de datos numéricos.
- Indivisible: los datos de obtendrá en el nivel más bajo.

- Definición: tienen que estar bien documentadas de todas sus características (frecuencia, indicadores, etc.)

- Usable: los resultados sirven para la toma de decisiones.

- Verificable: las revisiones deben de ser capaz de valorar el dato y obtener resultados.

- Estratégico: tiene que estar en relación con la misión y la estrategia de la seguridad de la información.

- Razonable: el valor del dato obtenido no tiene que ser mayor al coste de recolectarlo.

- Tendencia: los datos deberían de ser representar el impacto cuando se realizan cambios.

A la hora de seleccionar los controles necesarios la entidad tiene que hacer los siguientes pasos:

- Definir un programa.

- Seleccionar los controles y objetivos de control para ser incluidos en dichas mediciones.

- Definir los indicadores para sus respectivos controles.

6.7Plan-Do-Check-Act (PDCA)

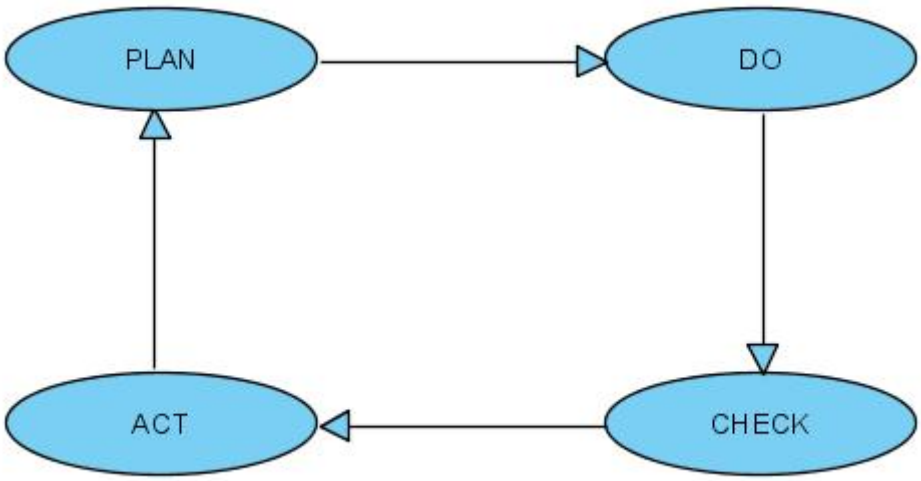
Consiste en una relación cíclica de entrada y salida de las actividades de medición. Las cuales se dividen en cuatro etapas.

- Plan

- Do

- Check

- Act



En este ciclo PDCA (Plan-Do-Check-Act), hay que tener mucho cuidado en cada nivel y tratarlo de forma cuidadosa desde el principio de su desarrollo ya que se van tomando una información totalmente necesaria a la hora de la toma de decisiones para la entidad y un pequeño error en ellas puede ocasionar graves problemas para la entidad. Ya que pueden arrastrar los errores una tras otra. Por lo tanto serán necesarias comentarlas una por una.

PLAN	Definir las metricas y establecer el sistema de gestión de seguridad de la informacion (SGSI)
DO	Adaptar procedimientos y controles para la obtención de datos
CHECK	Revisión de los datos obtenidos de las métricas realizadas
ACT	Revisión y mejora de las métricas de seguridad

Ahora las comentaremos a continuación las cuatro etapas de forma más exhaustiva:

PLAN: consiste en establecer SGSI y definir las métricas, en este punto para que la métrica que estemos definiendo para la seguridad sea correcta tiene que cumplir una serie de puntos necesarios para ello.

- Tiene que ser algo notable para la entidad en la cual se va a realizar.
- Tiene que poder medir la evolución de la seguridad en la entidad en el paso del tiempo (cambios, mejoras)
- Tiene que ser reproducible.
- Tiene que ser objetiva.
- Tiene que ser justificable
- Tiene que ser imparcial.

Una vez elegida la medida de seguridad hay que elegir la estrategia de seguridad que haya sido elegida por la alta dirección de la entidad mediante una serie de objetivos estratégicos.

Esta serie de objetivos estratégicos tienen una serie de indicadores los cuales tienen como función medir el grado o calificación que se obtiene a cumplir el objetivo. Dichos indicadores deberán de ser capaces de obtener una meta asociada que consiste en el valor que tienen que alcanzar los indicadores.

Sin embargo a la hora de elegir las métricas hay que pensar que los recursos de la entidad son limitados, lo que obliga a que solo se puedan realizar las métricas que sean rentables a la entidad, además hay que tener cuidado porque puede ser una arma de doble filo ya que si aplicamos más recursos de los debidos a dichas métricas de seguridad puede provocar grandes pérdidas a la entidad y acabar siendo un gran error en vez de ser un fortalecimiento para nuestra entidad, por lo tanto a la hora de elegir la métrica correcta tendremos que justificar los recursos utilizados junto al esfuerzo realizado con la información resultante que obtengamos, ya que si gastamos muchos recursos y esfuerzos para una obtener una información que no sea lo bastante valiosa para justificar tanto esfuerzo no habrá valido la pena ya que habrá producido más gastos de los necesarios para obtener dicha información y será una pérdida de tiempo, recursos y esfuerzo que traducido literalmente para la entidad consistirá en una gran pérdida de dinero para la entidad.

DO: consiste en adaptar procedimientos y controles con el fin de poder obtener los datos necesarios.

En este punto es necesaria la existencia del personal de trabajo para obtener, procesar y comunicar los datos obtenidos al cuadro de mando. Esto obliga que dicho personal tiene que estar cualificado para ello y por tanto dicho personal tiene que estar formado y concienciado a los trabajadores a la hora de evaluar dichos datos, ya que entonces podemos estar cometiendo un grave error a la hora de evaluar por parte del personal de la empresa y tener unos datos erróneos, por tanto para la empresa consistirá en dar un trabajo adicional a dichos trabajadores formándoles a la vez de invertir más dinero en ellos (pagar horas extras a los trabajadores por la formación) así como invertir en los recursos.

Estas personas que están tomando los datos tendrán que avisarlo de forma continua al cuadro de mando. Ya que gracias al cuadro de mando visualizaremos los datos obtenidos así como los resultados con el fin de ayudar a la mejora de la entidad y a ellos mismos a la hora de realizar su trabajo.

CHECK: en este punto tendremos que revisar los datos obtenidos de las métricas realizadas.

Este también es un punto importante ya que a la hora de las decisiones que tome una entidad se basan en relación a sus datos obtenidos y por tanto dichos datos no pueden ser erróneos ya que entonces tomarán decisiones a partir de una base la cual no es real o está equivocada debido a los datos tomados erróneamente, por tanto en este punto se centra en revisar los datos obtenidos de las métricas para que la entidad sepa realmente lo que está ocurriendo.

Para realizar la revisión de dichos datos se hará después de que los indicadores han sido implantados en la entidad. Consiguiendo así poder saber si dichos indicadores son rentables y útiles para la entidad.

Por último además de revisar los datos cogidos se recomienda también tomar nota de las opiniones de los empleados que usan dichos indicadores ya que toda información es necesaria, y posiblemente se necesiten varios puntos de vista a la hora de enfrentarse a un problema.

ACT: Este último punto se centra en la revisión y mejora de las métricas de seguridad.

Ahora se centrarán en las revisiones de la calidad de las métricas y de los objetivos con el fin de comprobar que siguen cumpliendo con los objetivos definidos en el principio además de que sigan siendo útiles para la entidad.

Cuando se realizan dichas revisiones tienen que comprobar y por tanto realizar una serie de puntos para comprobar que siguen siendo útiles. Los cuales son los siguientes:

- Tienen que evaluar la eficiencia del SGSI (sistema de gestión de seguridad de la información.

- Saber que el coste de mantener las métricas y la obtención de datos no sea superior al valor que aporta dicha información.

- Indicar la evolución de los objetivos de seguridad indicados por la entidad.

- Saber que los objetivos de las métricas no sean lo suficientemente bajos porque entonces siempre saldría de forma correcta.

Según vaya pasando el tiempo y el sistema de gestión de seguridad de la información vaya a la par madurando las métricas que tienen irán cambiando según pasa el tiempo y el sistema de gestión de seguridad de la información madure provocando que dichas métricas se modifiquen, se crean nuevas, o se eliminen. Es decir que indicadores que ahora pueden servirnos completamente con el paso del tiempo pueden dejar de ser útiles.

6.8Cuadro de mando

6.8.1¿Qué es un cuadro de mando?

Un cuadro de mando es una herramienta de gestión.

Al cuadro de mando se le considera como una de las herramientas más importantes, valiosas y potentes que puede utilizar la dirección de la entidad para evaluar su estado de seguridad el cual les servirá para la toma de decisiones.

Dicha herramienta deberá centrarse en los indicadores de la organización los cuales no cumplen los límites elegidos por la entidad así como los indicadores que pueden llegar a superar los límites elegidos.

Además el cuadro de mando tiene otras funciones como por ejemplo ayudar a la comunicación entre diferentes niveles de los empleados de la entidad, también sirve para asignar responsabilidades a dichos empleados.

También el cuadro de mando ayudará a la entidad a la hora de afrontar nuevos riesgos de seguridad, así como gestionar dichos controles de seguridad, cómo se percibe la seguridad por parte de los clientes, accionistas y empleados de la entidad y la más importante a contribuir a la hora de obtener los objetivos de negocio de la entidad.

El objetivo principal del cuadro de mando consistirá en mejorar los resultados que obtiene la entidad.

6.8.2¿Cómo implantar un cuadro de mando correcto en nuestra entidad?

Para la implantación de un cuadro de mando de seguridad es un trabajo con bastante dificultad desde el punto de vista organizativo y técnico. Esto provoca que en muchos casos dicho proyecto fracase en su implantación.

A la hora de implantar un cuadro de mando en nuestra entidad tendremos que tomar en cuenta ciertos puntos y aspectos con el fin de que la implantación sea de forma correcta y sin causar pequeños problemas en la entidad.

Para ello se recomienda que se cumplan las siguientes acciones:

- Señalar toda la información que sea totalmente necesaria de una forma resumida, sin complicaciones, entendible, sencilla y eficaz, todo esto servirá para la toma de decisiones.

- Resumir la representación usando un juego de colores el cual nos sirva para indicar los cambios de estado. (Rojo, amarillo, verde)

- Encadenar los indicadores a sus respectivos objetivos, con el fin de saber qué es lo que se está midiendo.

- Deberá de facilitar el trabajo de comparar resultados entre áreas de la entidad diferentes.

- Señalar lo importante para la compañía indicando aquellos indicadores que no evolucionan según era lo planificado por la entidad.

- Y el más importante de todos obtener el apoyo de la Dirección y alcanzar el mayor consenso posible entre los participantes del diseño.

Por último tenemos que señalar que dependiendo de a quien esté dirigido el cuadro de mando, los indicadores se agruparán de manera diferente dependiendo de los empleados que los utilizan.

- Si está centrado en la Dirección de la entidad habrá que realizar un cuadro de mando de valoración económica de los impactos técnicos para la entidad.

- Si está centrado en los empleados técnicos de la entidad se tendría que hacer un cuadro de mando de impacto de fallos técnicos.

6.9 Dirección

La dirección se encarga de mantener y establecer acuerdos de sus mediciones. La implementación tiene que estar de acuerdo a lo que indican los estándares internacionales, centrándose en la aceptación de los requerimientos de mediciones.

- Cualquier tipo de acuerdo será comunicado a la entidad de inmediato.

- Existirán acuerdos entre el personal que realiza las actividades de medición y la dirección, con el fin de demostrar que existe un interés de todas las áreas de la entidad.

Además la dirección tiene que hacer indicaciones de dichos acuerdos, de su operación, revisión, implementación, mantenimiento, mejora y monitorización del programa de mediciones mediante el uso de:

- Creación de uso de responsabilidades y roles.

- Comunicación de todo el personal que está involucrado en los indicadores de progreso y programa de mediciones.

- Comprobar que el programa se lleve a cabo.

- Que las revisiones de dicho programa sean parte del Sistema de Gestión de Seguridad de la información

- Se tiene que establecer el programa de mediciones.

- Comprobar que las auditorías internas que se realizan en relación al programa de mediciones sean correctas.

- Tener los recursos suficientes para llevar a cabo el programa de mediciones.

También la dirección está encargada de proveer y asignar los recursos necesarios para dicho programa de mediciones, ya sea desde recursos materiales para llevar sus funciones como del personal necesario para llevarlo a cabo.

La dirección asignará las siguientes responsabilidades y roles para la medición y ejecución de dicha medición los cuales son los siguientes:

- Personal responsable de los requerimientos de mediciones.
- Propietario de la medición.
- Personal que dirige e interviene en el programa.
- Personal responsable de la evaluación del programa.
- Personal responsable de almacenar y recolectar los atributos.
- Personal responsable de la comunicación a la entidad, sobre la importancia del programa de medición así como de sus resultados.

Para finalizar hay que recalcar que será de vital importancia realizar, acreditaciones, autorizaciones al personal que realizará los criterios y estas tareas para la formación técnica de los mismos. Hay que inculcar al empleado que son de vital importancia ya que contribuyen a la mejorar de los objetivos del Sistema de Gestión de la Seguridad de la Información.

6.10Explicacion detallada de la normativa

6.10.1. Visión General de Medición de la Información de la seguridad.

6.10.1.1 Objetivos de la medición de la seguridad de la información.

Los objetivos de medición de la seguridad de la información en relación con el Sistemas de Gestión de Seguridad de la Información incluyen:

a) Evaluar la eficacia de los controles aplicados o grupos de controles.
b) Evaluar la eficacia de la aplicación SGSI.
c) Verificar el grado en el que se fijaron las necesidades de seguridad y saber si han sido cumplidas.
d) Facilitar la mejora del rendimiento de la seguridad de la información en cuanto a los riesgos de negocio de la organización global.
e) Proporcionar información para la revisión por parte de la dirección para facilitar la toma de decisiones relacionadas con el Sistema de Gestión de Seguridad de la Información y justificar la necesidad de mejora de la aplicación del Sistema de Gestión de Seguridad de la Información.

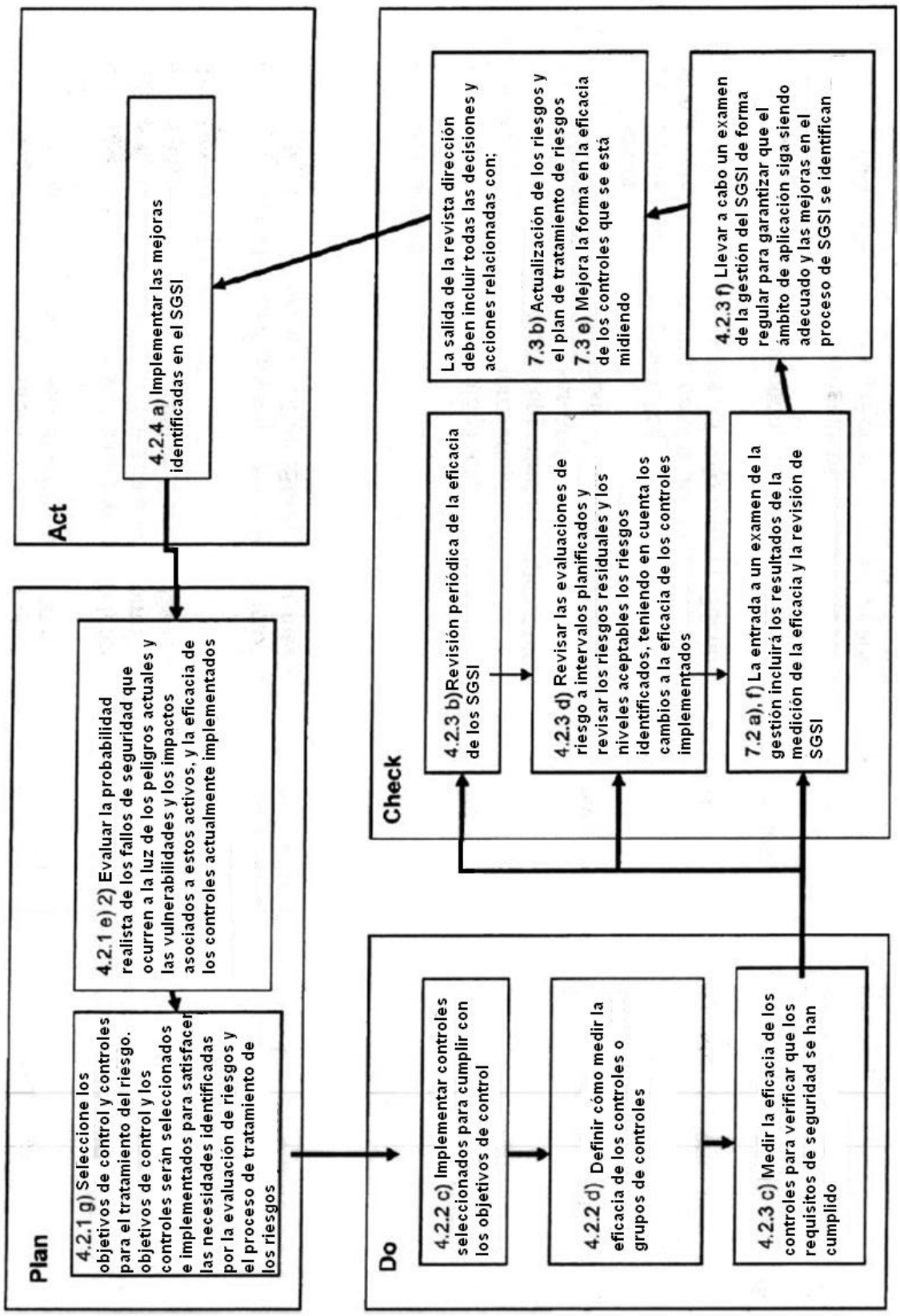


Figura 1-Medida entradas y salidas en el ciclo de SGSI PDCA de la gestión de seguridad de la información.

La organización deberá establecer los objetivos de medición basados en una serie de consideraciones:

a) El rol de la seguridad de la información en apoyo de actividades generales y de riesgos de la organización empresarial.

b) Los requisitos legales aplicables, reglamentarios y contractuales.

c) La estructura organizacional

d) Costos y beneficios de implementar medidas de seguridad de la información

e) Los criterios de riesgo de aceptación de la organización

f) La necesidad de comparar varios Sistemas de Gestión de Seguridad de la Información dentro la misma entidad, ya que pueden comparar con anteriores SGSI que han sido utilizados por la entidad usándolos como referencia.

En este punto vemos la utilización del PDCA, como ciclo, en el cual forma parte a la hora de cumplir todos los objetivos, como guía.

6.10.1.2 Programa de la seguridad de medición de la información

Una organización debe establecer y administrar un programa de seguridad de la información de medición para poder alcanzar los objetivos de medición establecidos y adoptar el modelo PDCA dentro de la organización global de las actividades de medición.

Ya que el modelo PDCA sirve de apoyo como estructura a la entidad en relación con las actividades que se realizan en la medición.

La organización también debería aplicar y desarrollar la medida construida con el fin de obtener objetivos y resultados útiles de medición basados en el modelo de la Seguridad de la Información de medición.

El programa de la gestión de la seguridad de la información y el desarrollo de la medición deben velar por la construcción de una organización eficaz para lograr medir de manera reproducible y objetiva, para proporcionar la medida de los resultados de las partes interesadas para determinar las necesidades para la mejora del SGSI implementado, incluyendo su alcance, políticas, objetivos, controles, procesos y procedimientos.

El programa de la seguridad de información de la medición debe incluir los siguientes procesos:

-Medidas y medición de desarrollo

-La operación de medición

a) El análisis de datos y medición de informar los resultados

b) Evaluación y mejora del programa de la seguridad de medición de la información.

La estructura organizativa y operativa del programa de la seguridad de medición de la información debería ser determinada teniendo en cuenta la escala y la complejidad del SGSI. En todos los casos, los roles y responsabilidades para el programa de la medición de seguridad de la información será asignada al personal competente.

En este punto es totalmente necesario (por no decir obligatorio, ya que ninguna norma obliga, solo aconseja) la existencia de un programa de medición con sus respectivos procesos creado por la propia entidad, con el fin de llegar a obtener sus objetivos.

6.10.1.3 Factores de éxito.

Los siguientes puntos a continuación son algunos de los factores que contribuyen al éxito del programa de la medición de seguridad de la información para facilitar la mejora continua del SGSI:

a) Compromiso de la gerencia con el apoyo de los recursos apropiados.

b) Existencia de procesos y procedimientos SGSI.

c) Un proceso repetible capaz de capturar y presentar informes para proporcionar datos significativos sobre las tendencias pertinentes a un periodo de tiempo.

d) Medidas cuantificables sobre la base de objetivos SGSI.

e) Datos fáciles de obtener que se pueden utilizar para la medición.

f) Evaluación de la efectividad de la seguridad de la información y de la medición de la aplicación de mejoras identificadas.

g) Recogida periódica de análisis y reporte de datos de medición de una manera más significativa.

h) Aceptación de información sobre los resultados de medición de las partes interesadas pertinentes

i) Las evaluaciones de la utilidad de los resultados de las mediciones y la implementación de las mejoras identificadas

Una vez realizado con éxito, un programa de medición de la seguridad de la información puede:

1) Demostrar el cumplimiento de una organización con los requisitos legales aplicables o reglamentarios y obligaciones contractuales

2) La identificación a los problemas de seguridad no detectadas previamente

3) Ayudar a los informes de gestión satisfacción de las necesidades al afirmar medidas por razones históricas y actividades actuales.

4) Ser utilizados como materia prima en proceso de seguridad de la información de gestión de riesgos, auditorías internas, y SGSI con revisiones por la dirección.

Como cualquier factor de éxito la mayor importancia que hay que tomar consiste en no tener ningún error a la hora de la realización del programa de la medición y que todos sus procesos se realicen de forma eficiente.

6.10.1.4 Modelo de medición de la seguridad de la información

6.10.1.4.1 Información general

El modelo de medición de la seguridad de la información consiste en ser una estructura que une una necesidad de información de los objetos relevantes de medida y sus atributos. Objetos de medición pueden incluir planificación o de ejecución de procesos, procedimientos, proyectos y recursos.

El modelo de medición de seguridad de la información se describe cómo los atributos relevantes son cuantificados y convierte a los indicadores que proporcionan una base para la toma de decisiones.

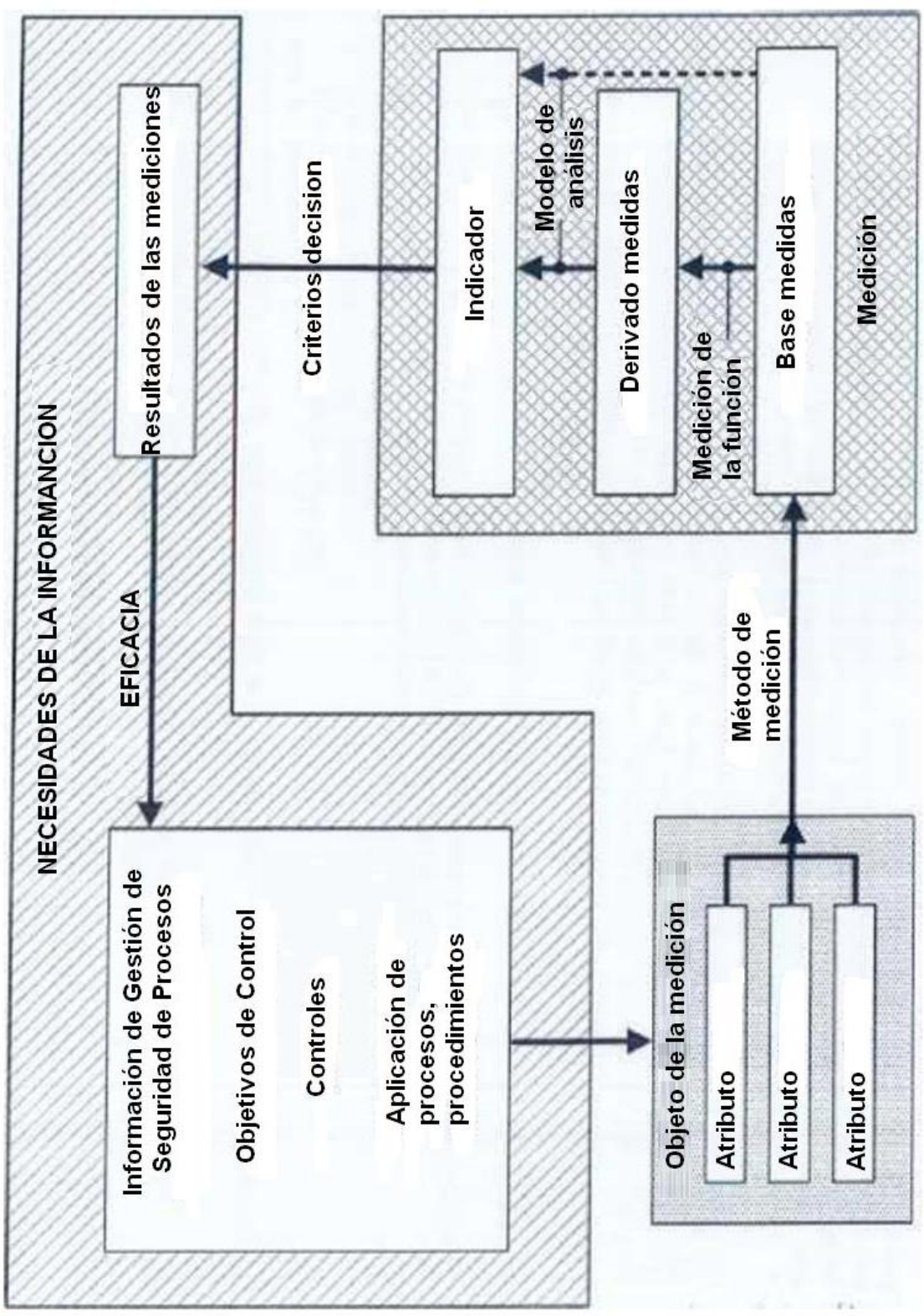


Figura 2 modelo de medición de seguridad de la información.

6.10.1.4.2 Base de medida y método de medición

Una medida base es la medida más sencilla que se puede obtener. Una medida base de los resultados de la aplicación es un método de medición de los atributos seleccionados de un objeto de la medición.

Un objeto de medición puede tener muchos atributos, sólo algunos de los cuales pueden proporcionar valores útiles para ser atribuido a un acto de base. Un determinado atributo puede utilizarse para varias medidas de base diferentes.

Un método de medición es una secuencia lógica de operaciones, utilizadas en la cuantificación de un atributo con respecto a una escala especificada. Las operaciones pueden incluir actividades tales como contar sucesos u observando el paso del tiempo.

Un método de medición puede utilizar los objetos de medición y los atributos de una variedad de fuentes, tales como:

-Análisis de riesgos y resultados de evaluación de riesgos;

-Cuestionarios y entrevistas personales;

-Informes de auditorías externas o internas;

-Los registros de los acontecimientos, las estadísticas de informes y de auditoría;

-Informes de incidencias, en particular las que dan lugar a la ocurrencia de un impacto;

-Resultados de los ensayos, la ingeniería social, herramientas para el cumplimiento, y las herramientas de auditoría de seguridad; o

-Los registros de los procedimientos de la organización seguridad de la información y programas relacionados.

Las tablas a continuación presentan la solicitud del modelo de seguridad de información para los siguientes controles:

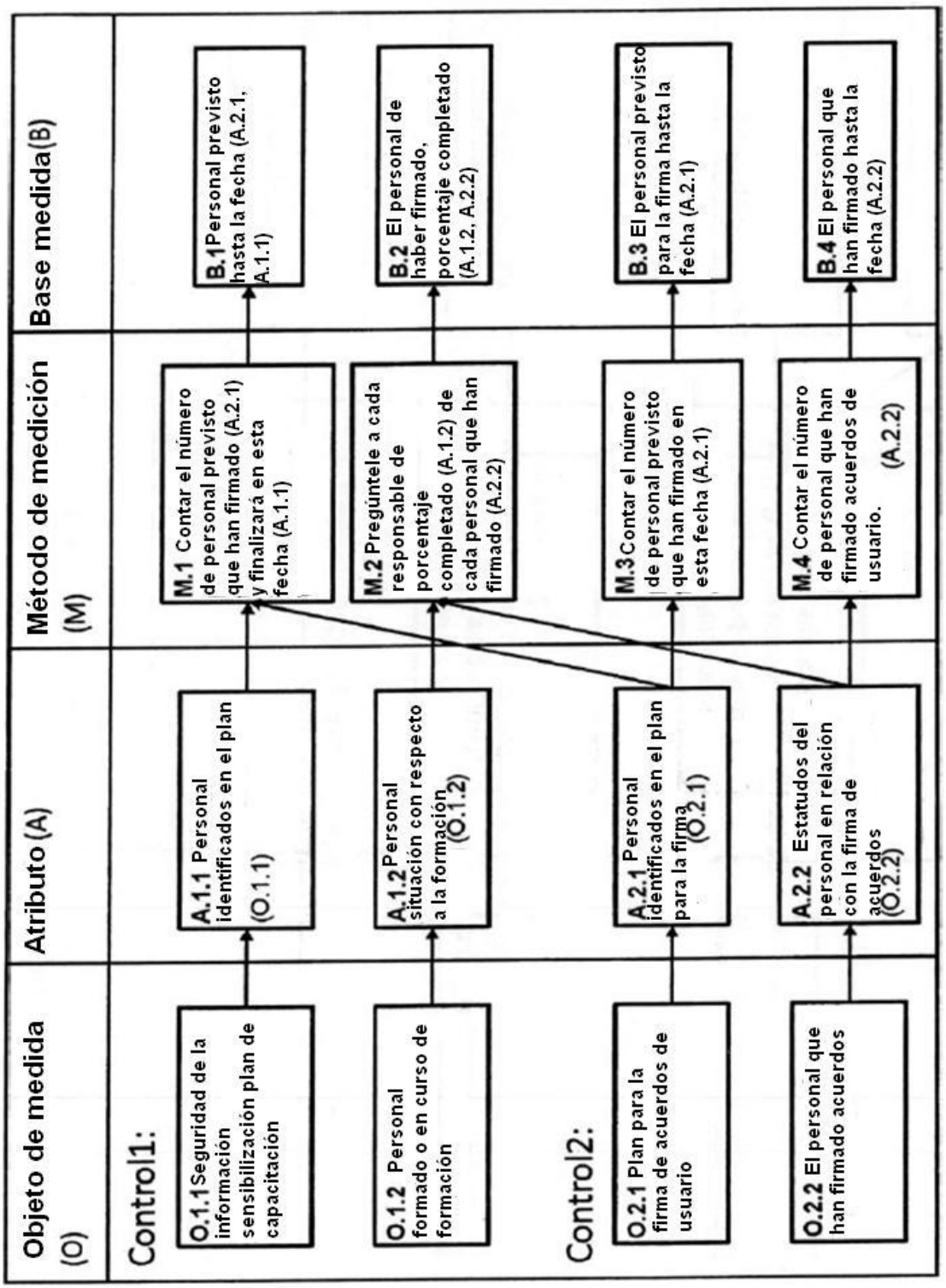
- "Control 2" hace referencia al control A.8.2.1 responsabilidad de la Dirección de la norma ISO / IEC 27001: 2005 ("Gestión exigirá a los empleados, contratistas y usuarios de terceras partes aplicar la seguridad de conformidad con políticas y procedimientos establecidos de la organización "); se aplica como sigue: "Todo el personal pertinente para el SGSI debe firmar acuerdos de usuario antes de acceder a un sistema de información";

- "Control 1" se refiere al control A.8.2.2 "acerca de la seguridad de la información, la educación y la formación" de ISO / IEC 27001: 2005 ("Todos los empleados de la

organización y, en su caso, los contratistas y terceros usuarios de las partes deberán recibir una formación adecuada toma de conciencia y actualizaciones regulares en las políticas de organización y procedimientos, lo concerniente a su función de trabajo"); se aplica como sigue: "Todo el personal relevante para el SGSI debe recibir formación sobre sensibilización y seguridad de la información antes de su concesión del acceso a un sistema de información ".

Hay que indicar que en relación a una medida base cuando se vaya a recoger tiene que ser simple y lo más importante tiene que tener una relación en referencia al método de medición, ya que si no se cumple no servirá de nada.

Tabla 1 incluye un ejemplo de las relaciones entre el objeto de la medición, el atributo, el método de la medición y la medida de base para medir los objetos establecidos para el control implementado descrito anteriormente.


Objeto de medida (O)
Atributo (A)
Método de medición (M)
Base medida(B)
Control1:
O.1.1Seguridad de la información sensibilización plan de capacitación
O.1.2 Personal formado o en curso de formación
A.1.1 Personal identificados en el plan (O.1.1)
A.1.2Personal situación con respecto a la formación (O.1.2)
M.1 Contar el número de personal previsto que han firmado (A.2.1) y finalizará en esta fecha (A.1.1)
M.2 Pregúntele a cada responsable de porcentaje completado (A.1.2) de cada personal que han firmado (A.2.2)
B.1Personal previsto hasta la fecha (A.2.1, A.1.1)
B.2 El personal de haber firmado, porcentaje completado (A.1.2, A.2.2)
Control2:
O.2.1 Plan para la firma de acuerdos de usuario
O.2.2 El personal que han firmado acuerdos
A.2.1 Personal identificados en el plan para la firma (O.2.1)
A.2.2 Estatudos del personal en relación con la firma de acuerdos (O.2.2)
M.3Contar el número de personal previsto que han firmado en esta fecha (A.2.1)
M.4 Contar el número de personal que han firmado acuerdos de usuario. (A.2.2)
B.3 El personal previsto para la firma hasta la fecha (A.2.1)
B.4 El personal que han firmado hasta la fecha (A.2.2)

6.10.1.4.3 Medida derivada y función de medición

Una medida derivada es un agregado de dos o más medidas de base. Una medida base determinada puede servir como entrada aplicable a diversas medidas derivadas.

Una función de la medición es un cálculo utilizado para combinar las acciones de base para crear una medida derivada.

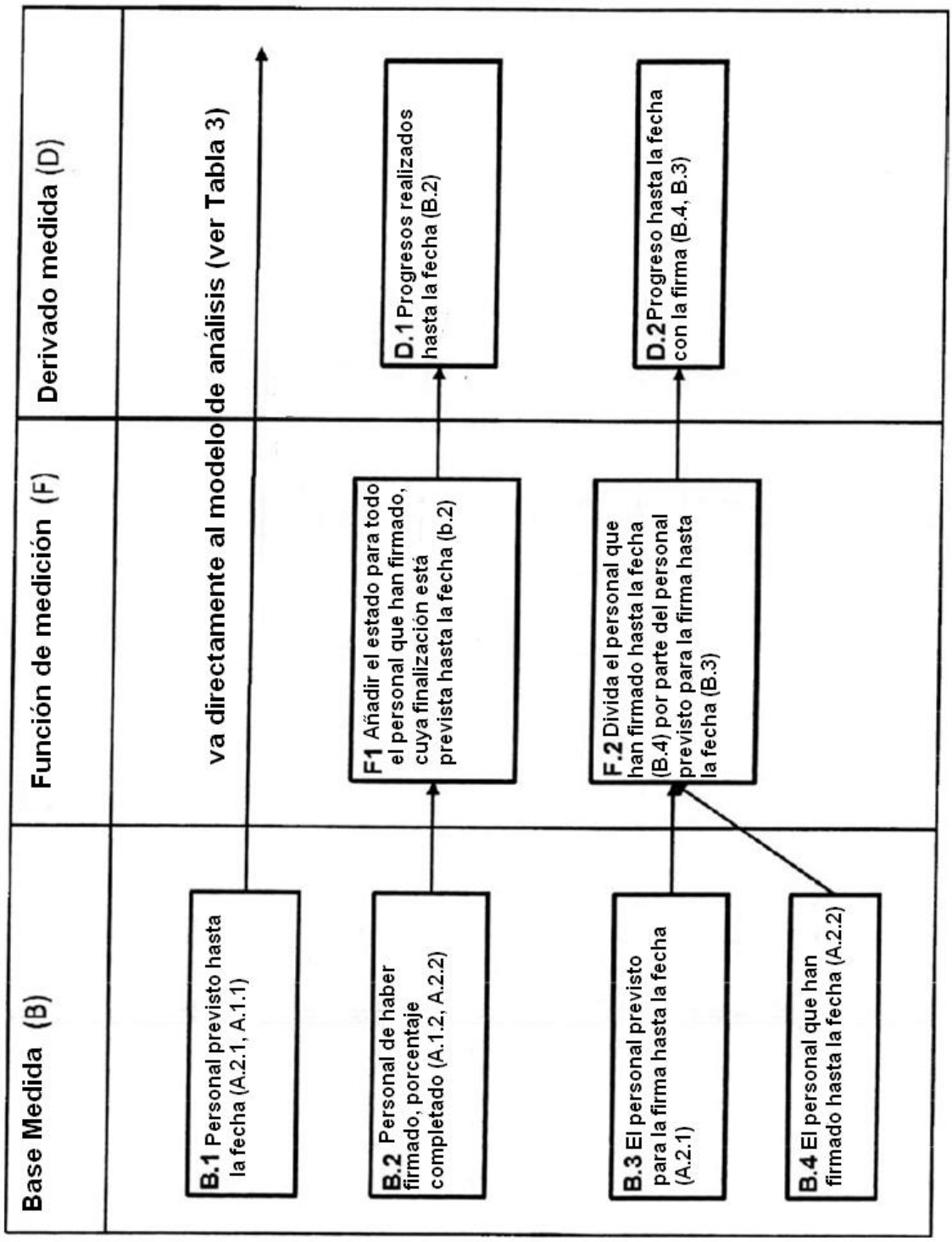
La escala y la unidad de la medida dependen de la escala derivada y unidades de las medidas de base desde la cual la componen, así como la forma en que se combinan la función de medición.

La función de medición puede implicar una variedad de técnicas, como promedio de medidas de base, aplicando pesos a las medidas de la base, o la asignación de valores cualitativos a las medidas de base.

La función de medición puede combinar medidas de base utilizando diferentes escalas, tales como porcentajes y los resultados cualitativos de evaluación.

Por supuesto a la hora de hacer una medida derivada tiene que existir una relación entre las medidas bases que se van a juntar con el fin de obtener nuestra medida derivada.

Un ejemplo de la relación de los elementos adicionales de la aplicación de seguridad de la información del modelo de medición medida base es decir, la función de medición y las ediciones obtenidas se presentan en la Tabla 2.



Cuadro 2-Ejemplo de medida derivada y la función de medición

6.10.1.4.4 Indicadores y el modelo analítico

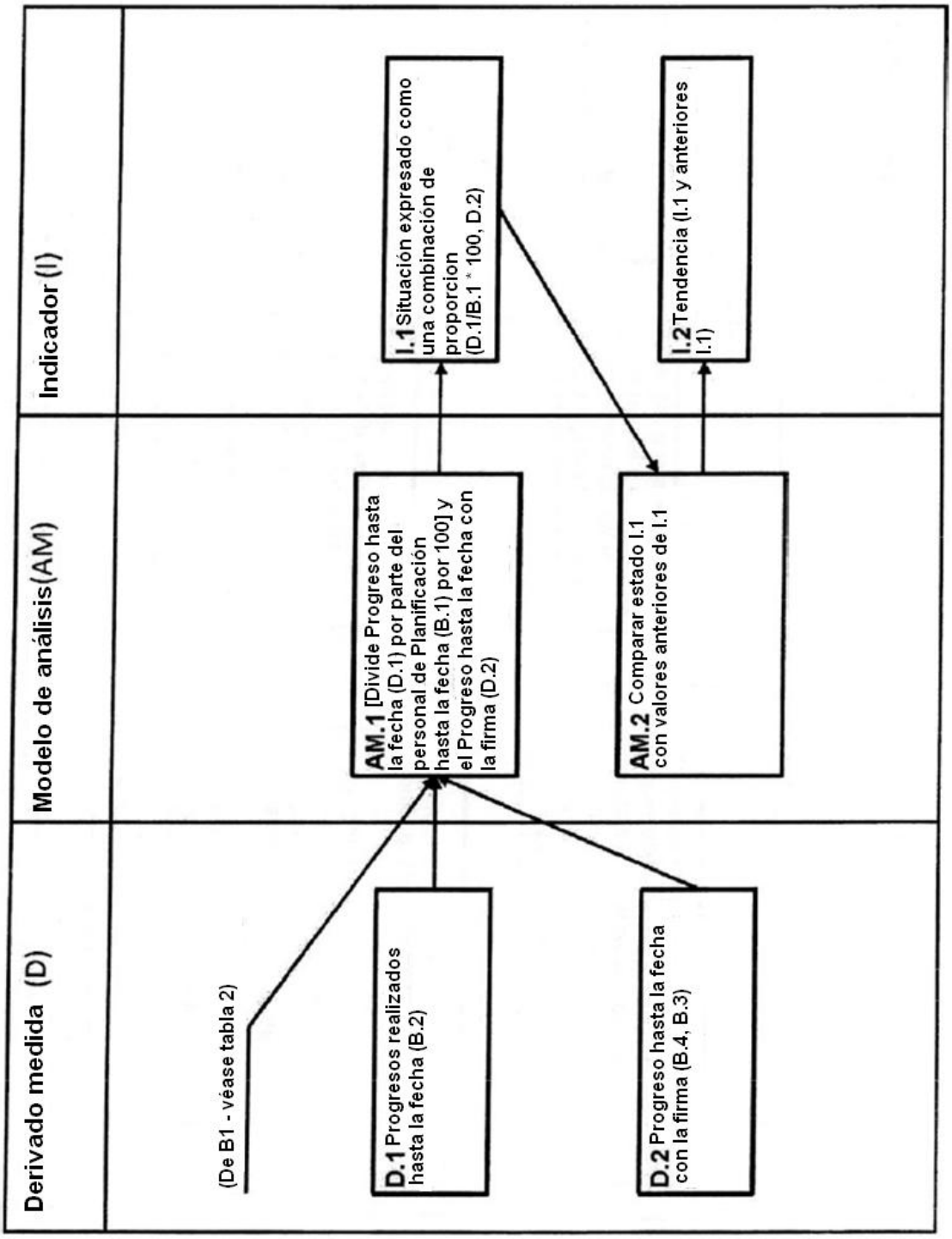
Un indicador es una medida que proporciona una estimación o evaluación de los atributos especificados derivados de una modelo de análisis con respecto a la necesidad de información definida. Los indicadores se obtienen mediante la aplicación de un análisis modelo a una base y / o una medida derivada y su combinación con los criterios de decisión.

Si un indicador está representado en una forma gráfica, debe ser utilizable por los usuarios con discapacidad visual. Para hacerlo posible la descripción de los indicadores debe incluir los colores, sombras, fuentes u otros métodos visuales.

La escala y el método de medición afecta a la elección de las técnicas analíticas utilizadas para producir indicadores.

Un ejemplo de las relaciones entre las medidas de derivados, el modelo de análisis e indicadores para la seguridad de la información de medición solicitud de modelo se presenta en la tabla 3.

Tabla 3-Ejemplo de indicador y modelo analítico


Derivado medida (D)
Modelo de análisis(AM)
Indicador (I)
(De B1 - véase tabla 2)
D.1 Progresos realizados hasta la fecha (B.2)
D.2 Progreso hasta la fecha con la firma (B.4, B.3)
AM.1 [Divide Progreso hasta la fecha (D.1) por parte del personal de Planificación hasta la fecha (B.1) por 100] y el Progreso hasta la fecha con la firma (D.2)
AM.2 Comparar estado I.1 con valores anteriores de I.1
I.1 Situación expresado como una combinación de proporcion (D.1/B.1 * 100, D.2)
I.2 Tendencia (I.1 y anteriores I.1)

6.10.1.4.5 Resultados de las mediciones y criterios de decisión

Los resultados de medición se desarrollan con la interpretación de los indicadores aplicables sobre la base de criterios de decisión se define y debe considerarse en el contexto de los objetivos de medición global de la evaluación de la eficacia del SGSI.

Los criterios de decisión se utilizan para determinar la necesidad de actuar o realizar otras investigaciones, así como a describir el nivel de confianza en los resultados de la medición. Los criterios de decisión pueden ser aplicados a una serie de indicadores, por ejemplo para realizar análisis de tendencias sobre la base de indicadores recibida en diferentes puntos en el tiempo.

El objetivo es proveer una especificación detallada de rendimiento, aplicable a la organización, derivados de los objetivos de seguridad de la información como los objetivos de SGSI y los objetivos de control, y que necesitan establecerse y reunirse para alcanzar dichos objetivos.

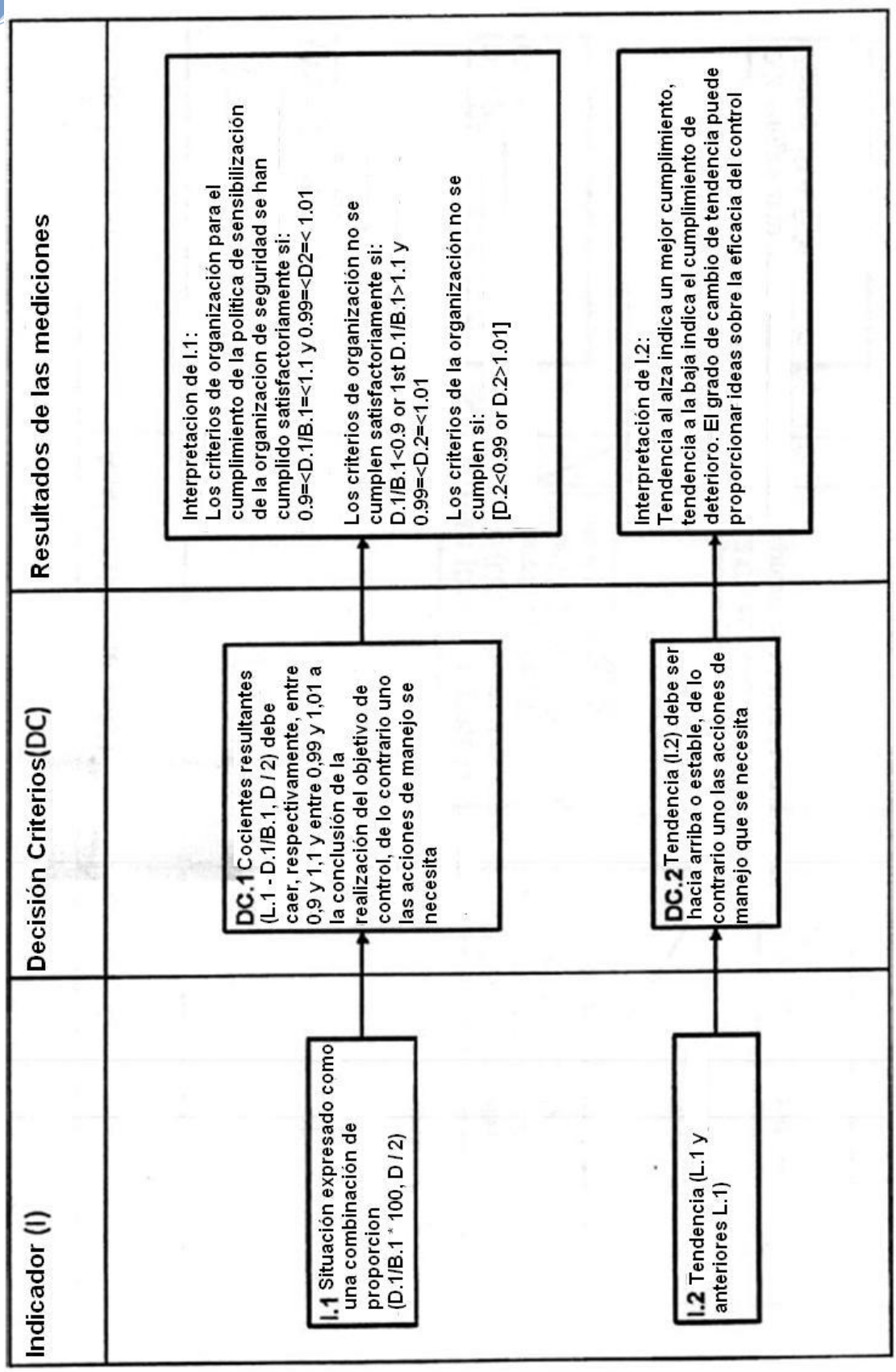


Tabla 4-Ejemplo de resultados de la medición y análisis del modelo

6.10.2 Gestión responsabilidades

6.10.2.1 Información general

La administración es responsable de establecer el programa de medición de seguridad de la información, con la participación de las partes interesadas pertinentes en las actividades de medición, la aceptación de los resultados de medición para el análisis de la gestión y el uso de medición de los resultados en la mejora de las actividades dentro del SGSI.

Para lograrlo, la dirección debería:

a) Establecer objetivos para el programa de información de seguridad de medición;

b) Establecer una política para el programa de información de seguridad de medición;

c) Establecer las funciones y responsabilidades en materia de programa de información de seguridad de medición;

d) Proporcionar recursos suficientes para llevar a cabo las medidas, incluida personal, la financiación, las herramientas e infraestructura;

e) Asegurar que los objetivos del programa de información de la seguridad de medición se cumplan;

f) Velar por que las herramientas y equipos utilizados (recursos) para recopilar los datos se mantienen correctamente;

g) Establecer el propósito de la medición para cada medida a construir;

h) Velar por que la medición proporciona información suficiente a las partes interesadas en relación con eficacia de los controles o el grupo de los controles y las necesidades para mejorar los controles aplicados.

En este caso para poder realizar dicha norma de forma correcta la administración tendrá que tomar sus propias responsabilidades para poder llevarlo a cabo de una forma correcta y sin errores.

6.10.2.2 Gestión de los recursos

La administración debe asignar y proporcionar recursos para apoyar las actividades esenciales de la medida, tales como recopilación de datos, análisis, almacenamiento, elaboración de informes y distribución. Las asignaciones de recursos deben incluir la asignación de:

a) Las personas con responsabilidad de todos los aspectos del programa de seguridad de la información de medición;

b) apoyo financiero adecuado;

c) apoyo a las infraestructuras adecuadas, tales como la infraestructura física y las herramientas utilizadas para realizar los procesos de medida.

Finalmente los recursos son totalmente necesarios para la medida aunque habrá que gestionarlos de manera eficaz para no ocasionar perdidas en la entidad cuando se utilizan dichos recursos.

6.10.2.3 Medición de formación, sensibilización y competencia

La administración debe garantizar que:

a) Las partes interesadas tengan una capacitación adecuada para el logro de sus funciones y responsabilidades en el programa de seguridad de la información de medición, y debidamente cualificado para desempeñar sus funciones y responsabilidades

b) Las partes interesadas entienden que sus deberes incluyen sugerencias para la mejora de la seguridad de la información aplicadas a la medición del programa.

6.10.3 Las medidas y la medición del desarrollo

6.10.3.1 Información general

Consiste en cómo desarrollar las medidas y mediciones para la elaboración de la evaluación de la eficacia de los SGSI implementados y el control de un grupo de controles, y la identificación específica de la organización del conjunto de medición de las construcciones. Las actividades necesarias para desarrollar las medidas y la medición deber de ser establecidos y documentados, incluyendo las siguientes:

a) Definir el alcance de medición;

b) La identificación de una necesidad de información;

c) Seleccionar el objeto de medición y sus atributos;

d) El desarrollo de la medición de las construcciones;

e) La aplicación de la medida de las construcciones;

f) El establecimiento de recogida de datos y procesos de análisis y herramientas

g) El establecimiento del método de medición ejecución y la documentación.

6.10.3.2 Definición de alcance de medición

Dependiendo de las capacidades de una organización y los recursos, el alcance inicial de la medición de una actividad de la organización se limita a elementos tales como controles específicos, los activos de información protegida por controles específicos, acciones específicas para la seguridad de la información que se concede la máxima prioridad por la administración. Con el tiempo, el alcance de las actividades de medición se amplió para hacer frente a otros elementos del SGSI implementado y los controles o grupo de controles, teniendo en cuenta las prioridades de los interesados.

Las partes interesadas deben ser identificadas y deben participar en la definición del alcance de medición. Los interesados pueden ser internos o externos a las unidades organizativas, tales como directores de proyectos, gestores de información del sistema, o los responsables de seguridad de información de decisiones. Los resultados específicos de medición abordar la efectividad de los controles individuales o un grupo de controles deben ser definidos y comunicados a las partes interesadas.

La organización puede considerar limitar el número de resultados de las mediciones que se informó a los responsables políticos dentro de un período de tiempo determinado para garantizar su capacidad para mejorar el efecto de SGSI basado en la informa resultados de las mediciones. Los resultados de medición debe ser priorizadas con base en la importancia de las necesidades de información correspondiente y los objetivos asociados de SGSI.

6.10.3.3 Identificación de la información necesaria.

Las siguientes actividades se deben realizar para identificar las necesidades de información pertinente:

a) Examinar el SGSI y sus procesos, tales como:

1) Política de SGSI y los objetivos, los objetivos de control y controles;

2) Legalidad, los requisitos contractuales y de organización de seguridad de la información;

3) La información de riesgos de seguridad los resultados del proceso de gestión, tal como se describe en la norma ISO / IEC 27001.

b) Dar prioridad a la información identificada, necesidades basadas en criterios, tales como:

1) Tratamiento de los riesgos y prioridades;

2) Las capacidades de una organización y los recursos;

3) Los intereses de las partes interesadas;

4) La política de seguridad de la información;

5) La información necesaria para cumplir los requisitos legales, reglamentarios y contractuales;

6) El valor de la información en relación con el coste de la medida;

c) Seleccionar un subconjunto de la información necesaria dirigida en la medición de las actividades de la prioridad lista,

d) Documentar y comunicar la información seleccionada a que todas las partes interesadas.

Toda información es necesaria siempre que no provoque una congestión de la información provocando retrasos para la entidad, además esta información tiene que ser correcta, breve y a tiempo.

6.10.3.4 Objeto y atributo de selección

Un objeto de medición y sus atributos deben ser identificados en el contexto general y el alcance de un SGSI. Cabe señalar que un objeto de medición puede tener varios atributos aplicables.

El objeto y sus atributos para ser utilizados por la medición deben ser seleccionados sobre la base de la prioridad de unas necesidades correspondientes de la información.

Los valores que se asignará a una medida de la base en cuestión se obtienen mediante la aplicación de una medida apropiada y un método para los atributos seleccionados. Este algoritmo de selección debe velar por que:

-Mediciones pertinentes y la base de un método de medición pertinente puedan ser conocidos,

-Resultados de la medición significativa pueden realizarse con base en los valores obtenidos y desarrollados medidas.

Características de los atributos seleccionados determinar qué tipo de un método de medición debe ser usado para obtener los valores que se asignarán a medidas de base (por ejemplo, cualitativa o cuantitativa).

Datos que describen el objeto de medida y los atributos correspondientes deben ser utilizados como los valores que sean asignados a las medidas de base. Ejemplos de objetos de medidas:

-Los productos y servicios;
-Procesos;
-Aplicable a activos tales como instalaciones, aplicaciones y sistemas de información.

Los atributos deberán ser revisados para garantizar que:

a) Que los atributos apropiados han sido seleccionados para la medición

b) La colección de datos se ha definido para que garantizar un número suficiente de atributos está presente para permitir una medición efectiva

Sólo los atributos que son relevantes para la medida de base correspondiente deben de ser seleccionados. Aunque la selección de los atributos debe tener en cuenta el grado de dificultad en la obtención de los atributos que mida, no debe hacerse únicamente en los datos que se obtienen fácilmente o el atributo de ser fácil de medida.

Cabe destacar que no todos los atributos de un objeto son necesarios a la hora de realizar las mediciones, algunos atributos pueden ser necesarios para una determinada medición o pueden ser para diversas mediciones, así como las existencias de atributos sin utilidad para las mediciones.

Ademas cualquier tipo de atributo u objeto deberá estar siempre documentado, así como las razones por las cuales han sido elegidos para la selección.

6.10.3.5 Medición de construir el desarrollo

6.10.3.5.1 Medida de selección

Las medidas que podrían satisfacer la necesidad de información seleccionada deben de ser identificadas. La identificación de las medidas debe establecerse de manera suficientemente detallada para permitir la selección de las medidas que deban aplicarse.

Las medidas identificadas que podrían satisfacer la necesidad de información seleccionada deben de ser seleccionadas.

Las medidas seleccionadas deben reflejar la prioridad de las necesidades de información. Otros criterios de ejemplo que pueden ser utilizados para la selección de medidas incluyen:

-La facilidad de recogida de datos;

-Disponibilidad de recursos humanos para recoger y gestionar los datos;

-La disponibilidad de herramientas adecuadas;

-Número de indicadores potencialmente relevantes con el apoyo de la medida de la base;

-Facilidad de interpretación;

-Número de usuarios de los resultados de medición desarrollados;

-Las pruebas de aptitud de la medida para el propósito y la información que necesita;

-Los costes de recogida, gestión y análisis de los datos.

Se puede realizar un listado de criterios por la entidad, como guía a la hora de tomar las medidas necesarias, en relación a un enfoque común.

6.10.3.5.2 Método de medición

Para cada medida básica individual un método de medición debe ser definido. Este método de medición es utilizado para cuantificar un objeto de la medición a través de la transformación de los atributos en el valor a asignar en la medida de base. Un método de medición puede ser subjetivo u objetivo. Los métodos subjetivos se basan en la cuantificación de participación de la opinión del empleado, mientras que el uso de métodos objetivos de cuantificación numérica basada en reglas como el recuento de lo que podrá llevarse a cabo a través de medios humanos o automatizados.

El método de medición cuantifica los atributos como valores mediante la aplicación de una escala adecuada. Cada escala utiliza unidades de medida. Sólo las cantidades expresadas en la misma unidad de medida están directamente comparables.

Para cada método de medición, el proceso de verificación debe ser establecido y documentado. Esta verificación debe garantizar un nivel de confianza en el valor que se obtendrá mediante la aplicación de un método de medición que un atributo del objeto de medición y atribuido a un acto de base.

Cuando sea necesario para determinar el valor válido, herramientas utilizadas para obtener los atributos deben estar normalizadas y verificadas en los intervalos especificados.

La precisión del método de medida se debe tomar en cuenta y la desviación asociada o variación deberá quedar registrado.

Un método de medición debe ser coherente en el tiempo de manera que los valores asignados a una medida tomada de base en diferentes momentos son comparables y que los valores asignados a una medida derivada y un indicador también son comparables.

6.10.3.5.3 Medición de la función

Para cada medida individual derivada de una función de medición deberá ser definida para que se aplique a dos o más los valores asignados a las medidas de base. Esta función de medición se utiliza para transformar los valores asignados a una o más medidas de base en el valor que se asigna a una medida derivada. En algunos casos, una base medida puede contribuir directamente al modelo analítico, además de una medida derivada.

Una función de medición (por ejemplo, un cálculo) puede implicar una variedad de técnicas, como promedio de valores asignados a las medidas de base, aplicar ponderaciones de los valores asignados a las medidas de base o de asignar valores cualitativos a los valores asignados a las medidas de base antes de agregar que en el valor que se asignará a un las mediciones obtenidas. La función de medición pueden combinar los valores asignados a las medidas de base utilizando diferentes escalas, tales como porcentajes y los resultados cualitativos de evaluación.

Por lo tanto se considera que la entidad debe de buscar nuevas funciones con el fin de obtener unos datos más precisos, puede existir un determinado grupo de personal de la entidad encargados en la búsqueda de estas nuevas funciones para ayudar a la entidad, deben de estar siempre intentado encontrar nuevos métodos.

6.10.3.5.4 Modelo de análisis

Para cada indicador, un modelo de análisis debe ser definido con el propósito de transformar uno o más valores asignados a una base y / o una medida derivada en el valor que se asigna a un indicador.

El modelo analítico combina medidas pertinentes en una forma que produce una salida que sea significativa para las partes interesadas.

La decisión sobre criterios que se aplican a un indicador también debe tenerse en cuenta al definir el modelo de análisis.

A veces un marcado modelo analítico puede ser tan simple como la transformación de un único valor asignado a una deriva medida en el valor que se asigna a un indicador.

6.10.3.5.5 Indicadores

Los valores que se asignarán a los indicadores serán producidos por la agregación de los valores asignados a la derivada medida e interpretación de estos valores en función de los criterios de decisión. Para cada indicador que se informará al cliente para la presentación formal de un indicador como parte de formatos de información debe definirse. Los formatos para la presentación del indicador deben ser personalizados para satisfacer las necesidades de información del cliente.

Todos los indicadores tendrán que estar documentados explicando en que consisten.

6.10.3.5.6 Criterios de decisión

Los criterios de decisión que corresponden a cada indicador deben ser definidos y documentados sobre la base de la información de los objetivos de seguridad, para orientar acciones concretas para los interesados. Esta orientación debe atender a las expectativas de progreso, y los umbrales para iniciar acciones de mejora basadas en el indicador.

Los criterios de decisión establecen un objetivo por el cual el éxito se mide y ofrecer orientación sobre interpretar el indicador en relación con su proximidad a la meta.
Los objetivos que deben fijarse para cada elemento con respecto al rendimiento de los procesos de SGSI y los controles, el logro de objetivos, y para la eficacia del SGSI a evaluar.

Una vez que las correcciones de las acciones basadas en los datos iniciales son identificados, los criterios adecuados de decisión y fases de aplicación se puede definir que sean realistas para un SGSI específico.

El establecimiento de criterios de decisión se puede facilitar si los datos históricos que se refieren a los países desarrollados o seleccionados están disponibles. Las tendencias

observadas en el pasado, dan una idea de los rangos de rendimiento que son existentes previamente y orientar la creación de criterios de decisión realistas. Los criterios de decisión pueden ser calculados o basados en una comprensión conceptual de comportamiento esperado. Los criterios de decisión pueden derivarse de datos históricos, planos, y la heurística, o calculado como el control de límites estadísticos.

6.10.3.5.7 Las partes interesadas

Para cada medida de las partes interesadas deben de ser identificadas y documentadas. Las partes interesadas pueden incluir los siguientes:

a) Para la medida del cliente: la gestión de otras partes interesadas que soliciten o requieran información sobre la eficacia de un SGSI, controles o grupo de controles;

b) Revisor de medición: la persona o unidad organizativa que valida que los países desarrollados con dicha medición de las construcciones son apropiadas para evaluar la eficacia de un SGSI, controles o de grupo de mando;

c) Propietarios de la información: la persona o unidad organizativa que posee la información acerca de un objeto de medición y atributos y es responsable de la medición;

d) Información del colector: la persona o unidad organizativa responsable de la recogida, registro y almacenamiento los datos

e) Información del comunicador: la persona o unidad organizativa responsable de los análisis de datos que tiene que comunicar los resultados de la medición.

La razón por la que hay que identificar y documentar reside en que todas ellas forman parte del programa de medición de seguridad de la información y por tanto hay que estar pendientes de ellas siempre.

6.10.3.6 Construcción de medición

Como mínimo, la construcción de medición especificada debe contener la siguiente información:

a) Objeto de la medición;

b) Objetivo de control que debe alcanzar los controles y controles específicos, el grupo de los controles y el proceso de SGSI a medir;

c) Objeto de la medición;

d) Datos que se recoge y se utilizan;

e) Los procesos de recogida de datos y análisis;

f) Proceso para la presentación de informes de resultados de las mediciones, incluidos los informes

g) Las responsabilidades de las partes interesadas pertinentes

h) Un ciclo de revisión de la medida para garantizar su utilidad en relación con una necesidad de información.

6.10.3.7 Reunión de datos, análisis y presentación de informes

Los procedimientos de recogida de datos y análisis, y los procesos de comunicación de los resultados de medición desarrollados deben de ser establecidos. Apoyo a herramientas, equipos de medición y tecnologías deben ser algoritmos establecidos, si es necesario. Estos procedimientos, herramientas, equipos de medición y tecnologías se dirigirán a las siguientes actividades:

a) La recopilación de datos, incluido el almacenamiento de datos y la verificación. Los procedimientos deben identificar cómo los datos se recogen mediante el método de medición, medición de la función y el modelo de análisis, así como el cómo y el dónde se almacenarán junto con toda la información de contexto necesaria para comprender y comprobar los datos. La verificación de datos puede hacerse mediante la inspección de los datos contra una lista de control que se construye para verificar que los datos que faltan son mínimos, y que el valor que se ha asignado a cada medida es válido.

b) Análisis de datos y presentación de informes de resultados de medición desarrollados. Los procedimientos deberán especificar las técnicas de análisis de datos, y la frecuencia, aspectos formales y los métodos para informar de los resultados de las mediciones. La gama de herramientas que pueden ser necesaria para realizar el análisis de datos deben ser identificadas.

Ejemplos de formatos de información son:

-Cuadros de mando para proporcionar información estratégica mediante la integración de los indicadores de alto nivel;

-La ejecución y la operación en el cuadro de mando menos centrada en los objetivos estratégicos y más vinculados a la eficacia de los controles y procesos específicos;

-Los informes, tales como una lista de medidas para un periodo de tiempo determinado, resúmenes de vinculación. Los informes se utilizan mejor cuando el usuario tiene que mirar a los datos en un formato fácil de leer,

-Los calibradores que representan un valor dinámico, incluidos las alertas, los elementos gráficos adicionales y etiquetado de criterios de valoración.

Todos estos elementos forman parte de la medición y son de vital necesidad con el fin de tener todo los detalles controlados.

6.10.3.8 Medición de la implementación y la documentación

El enfoque global de la medida debe ser documentado en un plan de implementación. La puesta en práctica debe incluir la siguiente información como mínimo:

a) El programa de la seguridad de la información de medición implementado para la organización;

b) Medición de la siguiente especificación:

1) La medición genérica de la construcción de la organización;

2) Medición individual de las construcciones de la organización,

3) Definición de la gama y los procedimientos de recopilación de datos y análisis de datos;

c) Plan de calendario para realizar las actividades de medición;

d) Los registros creados a través de actividades de medición, entre ellas los datos recopilados y los registros de análisis;

e) formatos de los informes de resultados de las mediciones que se comunique a la dirección y los agentes interesados

6.10.4 Medición de la operación

6.10.4.1 Información general

La operación de medida de seguridad de información incluye actividades que son esenciales para asegurar que los resultados obtenidos en la medición proporcionen información precisa con respecto a la eficacia de una aplicación SGSI, controles o grupo de controles y la necesidad de acciones de mejora apropiadas. Esta actividad incluye el texto siguiente:

a) La integración de los procedimientos de medición en el funcionamiento general del SGSI.

b) Reunir, almacenar y verificar los datos.

6.10.4.2 Procedimiento de integración

El programa de medición de seguridad de la información debe estar plenamente integrada y utilizada por el SGSI. El procedimiento de medición debe ser coordinado con el funcionamiento del SGSI, incluyendo:

a) Definición y documentación de las funciones, autoridad y responsabilidad, con respecto al desarrollo, implementación y mantenimiento de información de medidas de seguridad;

b) Recopilación de datos y, cuando sea necesario, que modifica el actual funcionamiento del SGSI para dar cabida a los datos actividades de generación y recolección;

c) Comunicación de los cambios en las actividades de recopilación de datos a las partes interesadas;

d) Mantenimiento de la competencia de recolectores de información y la comprensión de los tipos de datos requeridos, los datos herramientas de recolección y los procedimientos de recopilación de datos;

e) Desarrollo de políticas y procedimientos que definen el uso de la medida dentro de la organización, difusión de la información de medida, verificación y revisión de la Seguridad de la Información y Medición del Programa;

f) Integración de análisis de datos y presentación de informes en los procesos pertinentes para asegurar su funcionamiento regular;

g) El seguimiento, revisión y evaluación de resultados de la medición;

h) Establecimiento de un proceso de retirada de las medidas a cabo y la adición de nuevas medidas para garantizar su evolucionar con la organización

i) Establecimiento de un proceso para determinar el uso de vida de los datos históricos para análisis de tendencias.

Estos puntos nos sirven de guía a la hora de integrar el programa de medición en el SGSI, y a la hora de realizar dicho puntos encontraremos los posibles problemas en dicha integración.

6.10.4.3 Reunión de datos, almacenamiento y verificación

La recolección de datos, almacenamiento y actividades de verificación incluyen las siguientes:

a) Reunir los datos requeridos, dentro de los intervalos regulares a través de un método de medición designada;

b) La documentación de la recogida de datos, incluyendo:

1) Fecha, hora y lugar de reunión de datos;

2) Colector de la información;

3) Información del propietario;

4) Los problemas que surgieron durante la recogida de datos que pueden ser útiles;

5) Información para la verificación y medición de datos de validación

c) Verificación de los datos recogidos contra las medidas de los criterios de selección y medición de las construcciones de validación. Los datos recogidos y cualquier información de contexto necesaria deben ser consolidados y restaurados en una grabación formal conducentes al análisis de datos.

6.10.5 Resultados de análisis de los datos y la medición de presentación de informes

6.10.5.1 Información general

Los datos recogidos deben ser analizados para desarrollar los resultados de medición y resultados obtenidos en la medición deben ser comunicados. Esta actividad incluye:

a) El análisis de los datos y el desarrollo de resultados de la medición,

b) Comunicar resultados de las mediciones a las partes interesadas.

6.10.5.2 Análisis de los datos y desarrollo de los resultados de medición

Los datos recogidos deben ser analizados e interpretados en términos de los criterios de decisión. Los datos pueden ser agregados, transformados, o re-codificados antes del análisis. Durante esta tarea, los datos se procesan para producir los indicadores. Se puede aplicar un número de técnicas de análisis. La profundidad del análisis deberá ser determinada por la naturaleza de los datos y la necesidad de información.

Los resultados de análisis de datos deben ser interpretados. La persona que analiza los resultados (comunicador) debe ser capaz de extraer algunas conclusiones iniciales sobre la base de los resultados. Sin embargo, el comunicador puede no ser partícipe directamente en las conclusiones técnicas y procesos de gestión, y deben ser revisadas por otros las partes interesadas.

El análisis de datos debe identificar las brechas entre los resultados esperados y la medición real de una aplicación SGSI, controles o grupos de controles. Las brechas detectadas apuntarán a las necesidades para mejorar el SGSI en práctica, incluyendo su alcance, las políticas, objetivos, controles, procesos y procedimientos.

Los indicadores que demuestren el incumplimiento o mal desempeño deben ser identificados y se puede clasificar como sigue:

a) El tratamiento del riesgo para implantar o suficientemente implementar, operar y administrar los controles o procesos SGSI (por ejemplo, controles y procesos SGSI pueden pasar por alto las amenazas);

b) Falta de evaluación de riesgos:

1) Los controles o procesos SGSI son ineficaces porque no son suficientes para contrarrestar cualesquiera amenazas estimadas (por ejemplo, porque la probabilidad de las amenazas fue subestimada), o afrontar las nuevas amenazas;

2) Los controles o procesos SGSI no se aplican, debido a las amenazas por alto. Los informes que se utilizan para comunicar los resultados de medición a las partes interesadas deben estar preparados utilizando formatos apropiados de referencia, de conformidad con el plan de implementación del programa de seguridad de información de la medición.

Las conclusiones del análisis deben ser revisada por las partes interesadas para garantizar la correcta interpretación de los datos. Los resultados del análisis de datos deben ser documentados para la comunicación a los interesados.

6.10.5.3Comunicar los resultados de medición

El comunicador de la información debe determinar la forma de comunicar los resultados de la medida de seguridad de la información, tales como:

-¿Qué resultados de la medición se habrán de comunicar interna y externamente?;

-Listados de las medidas correspondientes a actores individuales, y las partes interesadas;

-Los resultados específicos de medición que deberán realizarse, y el tipo de presentación, adaptados a las necesidades de cada grupo,

- Medidas para recabar la opinión de los interesados que se utilizarán para evaluar la utilidad de resultados de la medición y la eficacia de Seguridad de la Información de medición.

Los resultados de medición deben ser comunicados a una variedad de grupos de interés internos incluyendo a:

-Clientes para la medición

-Información propietarios

-Personal a cargo de la gestión de la información de riesgos de seguridad, especialmente donde el fracaso de riesgo de evaluación sean conocido

-El personal responsable de las áreas identificadas en necesidad de mejoramiento.

La organización podrá solicitar, en algunos casos para distribuir informes de resultados de la medición a las partes externas, incluidas las autoridades reguladoras, accionistas, clientes y proveedores. Se recomienda que los informes sobre resultados de las mediciones que se distribuyan al exterior sólo contengan los datos apropiados para la liberación externa y sean aprobados por la administración y las partes interesadas antes de ser liberados.

El comunicador tiene una gran responsabilidad ya que las decisiones que tome para indicar que determinados resultados habrá que señalar internamente o externamente tendrán una gran influencia en la toma de decisiones.

6.10.6 Programa de medición de seguridad de la información de Evaluación y Mejora

6.10.6.1 Información general

La organización debe evaluar a intervalos planificados lo siguiente:

a) La eficacia de la aplicación de medición de seguridad de la información para asegurarse de que:

1) Produce resultados de medición de una manera eficaz;

2) se ejecuta según lo previsto;

3) los cambios de direcciones en el SGSI implementado y / o controles;

4) cambios de direcciones en el medio ambiente (por ejemplo, los requisitos, la legislación o la tecnología),

b) Utilidad de los resultados de medición desarrollados para garantizar que se satisfagan las necesidades de información pertinentes. La administración debe especificar la frecuencia de dicha evaluación, el plan de revisiones periódicas y

establecer los mecanismos para hacer posibles revisiones. Las actividades correspondientes que deben ser las siguientes:

1) Determinar los criterios de evaluación para la medición de la Seguridad de la Información;

2) Para supervisar, revisar y evaluar la medición,

3) Implementar mejoras

6.10.6.2 Criterios de evaluación de identificación del programa de medición de seguridad de la información

La organización debe definir los criterios para evaluar la eficacia del programa de medición de seguridad de la información, así como la utilidad de los resultados de medición desarrollados. Los criterios deben ser definidos en el comienzo del programa de medición de seguridad de la información, teniendo en cuenta los objetivos de negocio de la organización.

Los criterios más probables cuando las organizaciones deben evaluar y mejorar la seguridad de la información aplicadas al programa de medición son:

-Cambios en los objetivos de negocio de la organización;

-Los cambios en los requisitos legales o reglamentarios y las obligaciones contractuales en materia de seguridad de la información;

-Cambios en los requisitos de organización en materia de seguridad de la información;

-Los cambios en los riesgos de seguridad de la información a la organización;

-Mayor disponibilidad de datos más precisos o convenientes y / o métodos para recoger datos para la medición;

-Los cambios en el objeto de la medida y / o sus atributos;

Los siguientes criterios pueden aplicarse para evaluar los resultados de medición desarrollada

a) Los resultados de medición son:

1) Fáciles de entender;

2) Comunicados de manera oportuna

3) Objetivos, comparables y reproducibles.

b) Los procesos establecidos para el desarrollo de los resultados de medición son:

1) Bien definidos;

2) Facilidad de operación;

3) Seguidos correctamente.

c) Los resultados de medición son útiles para mejorar la seguridad de la información.

d) Los resultados de medición que corresponde atender a las necesidades de información.

6.10.6.3 Monitorizar, revisar y evaluar el programa de medición de seguridad de la información

La organización debe supervisar, revisar y evaluar su programa de medición de seguridad de la información con los criterios establecidos.

La organización debe identificar las necesidades de potencial de mejora de la medición de programa de Seguridad de la Información, incluyendo:

a) La revisión de las medidas adoptadas, o eliminar las construcciones que ya no son apropiadas,

b) Volver a la asignación de recursos para apoyar la seguridad de la información de medición.

La organización también debe identificar las posibles necesidades de mejora del SGSI, incluido su ámbito de aplicación, las políticas, objetivos, controles, procesos y procedimientos, y las decisiones de gestión de documentos para permitir la comparación y análisis de tendencias durante las revisiones posteriores.

Los resultados de esta evaluación y las necesidades identificadas de potencial de mejora deben ser comunicadas a las partes interesadas pertinentes para permitir la toma de decisiones relativas a las mejoras necesarias.

El programa de medición de seguridad de la información deberá estar siempre seguido por parte de la entidad desde sus inicios, con los cambios que se realicen durante su vida hasta el punto en que no sea de utilidad a la empresa y sea descartado. Ademas esto servirá de experiencia para futuros programas de medición de seguridad de la información que utilice la empresa ya que podrán compararlos en cualquier momentos con los anteriores utilizados, en caso de que quieran comprobar alguna diferencia.

6.10.6.4 Implementar mejoras

La organización debe asegurarse de que haya interesados en identificar las mejoras necesarias del programa de medición de seguridad de la información. Las mejoras identificadas deben ser aprobadas por la dirección. Los planes aprobados deben estar documentados y comunicados a los interesados que corresponda.

La organización debe asegurarse de que las mejoras aprobadas de la información de medida de seguridad del programa se están ejecutando según lo previsto.

La organización tendrá que estar buscando siempre la mejora continua.

6.10.7 PLANTILLAS

6.10.7.1 Plantilla base

A continuación pondremos una plantilla base para una medida de seguridad de la información a construir.

Identificación de la medición a construir	
Nombre de la medición de construcción	Nombre de la medición
Identificador numérico	Numero único de identificación numérico de la organización
Propósito de la medida a construir	Describir las razones para la realización de tal medición
Control/Proceso objetivo	Control/proceso objetivo bajo la medición
Control(1)/Proceso(1)	Control/proceso bajo medición
Control(2)/Proceso(2)	Opcional: otros controles y procesos incluidos dentro de la misma medición
Objeto de la medición y atributos	
Objeto de medición	Objeto (entidad) que se caracteriza a través de la medición de sus atributos. Un objeto puede incluir procesos, planes, proyectos, recursos y sistemas o componentes del sistema.
Atributo	Propiedad o característica de un objeto de la medición que se pueden distinguir cuantitativa o cualitativamente por medios humanos o

	automatizados.
Base medida de las especificaciones (por cada medida de referencia [1 .. n])	
Base medida	Una medida base es definida en términos de un atributo y el método de medición especificado para su cuantificación (por ejemplo: Número de personal capacitado, el número de sitios, el costo acumulado hasta la fecha). Como se recopilan los datos, se asigna un valor a una medida de base.
Método de medición	Secuencia lógica de las operaciones utilizadas en la cuantificación de un atributo con respecto a una escala determinada.
Tipo de método de medición	Dependiendo de la naturaleza de las operaciones utilizadas para cuantificar un atributo, dos tipos de método se pueden distinguir: -Subjetiva: cuantificación que entrañan juicios humanos. -Objetivo: cuantificación numérica basada en normas tales como contar.
Escala	Conjunto ordenado de valores o categorías a las que atribuyen la medida base.
Tipo de escala	Dependiendo de la naturaleza de la relación entre los valores de la escala, cuatro tipos de escala se definen habitualmente: nominal, ordinal, intervalo y proporciones.
Unidad de medida	Especial cuantificar, definido y aprobado por la convención, con la que cualquier otra cantidad de la misma clase se puede comparar a expresar la relación de las dos cantidades como un número.
Especificación de la medida derivada	
Medida derivada	Una medida que se deriva en función de las medidas de dos o más bases
Medición de la función	Algoritmo de cálculo de combinar dos o más medidas de base. La escala y la unidad de la medida derivados dependen de las escalas y las unidades de las medidas de base desde la cual se compone, así como la forma en que se combinan por la función
Especificación del indicador	

Indicador	Medida que proporciona una estimación o evaluación de los atributos especificados derivados de un modelo de análisis con respecto a una necesidad de información definida. Los indicadores son la base para el análisis y toma de decisiones
Modelo analítico	Algoritmo de cálculo o la mezcla de uno o más de base y / o las medidas derivadas de los criterios de decisión correspondiente. Se basa en el conocimiento de, o supuestos sobre la relación esperada entre la base y / o derivados de la medida y / o su comportamiento en el tiempo. Un modelo analítico produce estimaciones o las evaluaciones correspondientes a una necesidad de información definida
Especificación de los criterios de decisión	
Decisión criterios	Umbrales, objetivos, o patrones que se utilizan para determinar la necesidad de una acción o investigación, o para describir el nivel de confianza en un resultado dado. Criterios de decisión ayudarán a interpretar los resultados de la medición
Resultados de las mediciones	
Interpretación de indicador	Una descripción de cómo el indicador debe ser interpretado
Formatos de los informes	Formatos de los informes deben ser identificados y documentados. Describir las observaciones que la organización o el titular de la información desea. Formatos de presentación visual se describen las medidas y se da una explicación verbal de los indicadores. Los formatos de presentación de informes deben ser personalizados para el cliente.
Las partes interesadas	
Cliente para la medición	Gestión o de otras partes interesadas que soliciten o requieran información sobre la eficacia de un SGSI, controles o grupo de controles
Revisor para la medición	Persona o unidad organizativa que valida que la medición desarrollada es apropiada para evaluar la eficacia de un SGSI, controles o grupo de controles

Propietario de la información	Persona o unidad organizativa que posee la información acerca de un objeto de medición y los atributos y es responsable de la medición
Colector de la información	Persona o unidad organizativa responsable de la recogida, registro y almacenamiento de los datos
Comunicador de la información	Persona o unidad organizativa responsable de análisis de datos y de comunicar los resultados de la medición.
Frecuencia/periodo	
Frecuencia de la recogida de datos	¿Con qué frecuencia se recopilan los datos?
Frecuencia de análisis de datos	¿Con qué frecuencia se analizan los datos?
La frecuencia de presentación de informes resultados de las mediciones	¿Con qué frecuencia los resultados son presentados?
Medición de la revisión	Fecha de revisión de medida (de caducidad o renovación de medición de validez)
Periodo de medición	Define el periodo que se mide

6.10.7.2 Plantilla de ejemplo

A continuación vamos a poner una plantilla de ejemplo respecto al entrenamiento del personal del SGSI.

identificación de la medición a construir	
Nombre de la medición de construcción	SGSI – personal capacitado
Identificador numérico	Específico de cada organización
Propósito de la medida a construir	Para determinar el cumplimiento con la política de control de la organización de seguridad de la información
Control/Proceso de objetivos	Formación, sensibilización y competencia profesional
Control(1)/Proceso(1)	Formación, sensibilización y competencia profesional. La organización debe asegurarse de que todos los empleados a quien es se asignan responsabilidades definidas en el SGSI son competentes para realizar las tareas que corresponden a: d) llevar un registro o la educación, formación, habilidades, experiencia y calificaciones.
Control(2)/Proceso(2)	Opcional: nuevos controles dentro del grupo incluido en la misma medida en su caso (planificación o de ejecución)
Objeto de la medición y atributos	
Objeto de medición	Empleados de la base de datos
Atributo	Registros de entrenamiento
Base medida de las especificaciones (por cada medida de referencia [1 .. n])	
Base medida	Número de empleados que recibieron formación SGSI según el plan anual de capacitación SGSI. Número de empleados que tienen que recibir una formación SGSI

Método de medición	Cuenta de registros con el campo de entrenamiento SGSI / fila como relleno para indicar el estado de“Recibido”
Tipo de método de medición	Objetivo
Escala	Numérico
Tipo de escala	Proporción
Unidad de medida	Empleado
Especificación de la medida derivada	
Medida derivada	Porcentaje de ISMS - personal capacitado
Medición de la función	Número de empleados que recibieron formación SGSI / número de empleados que tienen que recibir una formación SGSI * 100
Especificación del indicador	
Indicador	El uso de un código de colores con colores identificadores. Gráfico de barras que representa el cumplimiento durante varios períodos de información en relación con los umbrales (rojo, amarillo, verde) definido por el modelo analítico. El número de los períodos de información que se utilizará en la tabla debe ser definida por la organización
Modelo analítico	0-60% - Rojo, Amarillo 60-90%; 90-100% Verde. Para el amarillo, si el progreso de al menos 10% por trimestre no se logra, número de forma automática rojo
Especificación de los criterios de decisión	
Criterios de decisión	Rojo - se requiere la intervención, el análisis de la causalidad debe llevarse a cabo para determinar las razones de incumplimiento y mal desempeño. Amarillo - indicador debe ser vigilado de cerca por el deslizamiento posible rojo. Verde - no requiere ninguna acción
Resultados de las mediciones	

Interpretación de indicador	Especifico de la organización
Formatos de los informes	Gráfico de barras con barras de colores sobre la base de criterios de decisión. Breve resumen de lo que significa la medida y las posibles medidas de gestión de atribuirse a la gráfica de barras
Las partes interesadas	
Cliente para la medición	Los gerentes responsables de un SGSI
Revisor para la medición	Los gerentes responsables de un SGSI
Propietario de la información	Gerente de Capacitación - Recursos Humanos
Colector de la información	Formación de gestión - departamento de recursos humanos
Comunicador de la información	Los gerentes responsables de un SGSI
Frecuencia/periodo	
Frecuencia de la recogida de datos	Mensualmente, primer día de mes
Frecuencia de análisis de datos	Trimestral
La frecuencia de presentación de informes resultados de las mediciones	Trimestral
Medición de la revisión	Revisión anual
Periodo de medición	Anual

7.CUESTIONARIO-APLICACION

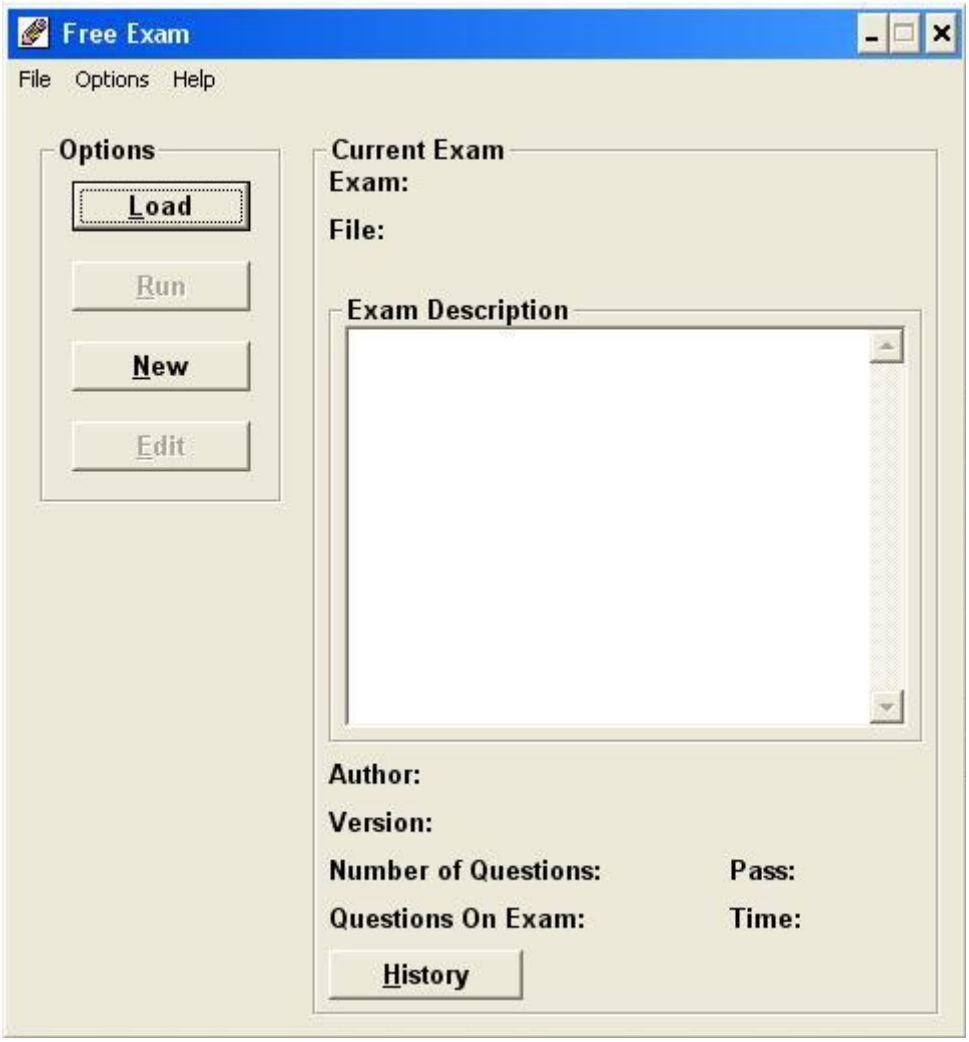
7.1 Introducción

Para ayudar a los auditores a la hora de la realización del cuestionario he partido del programa "Freeexam", con el cual el auditor podrá crear o modificar cualquier tipo de cuestionario, en caso de que tenga preguntas o respuestas ambiguas, en función de sus necesidades, etc.; además el programa soporta los test multirespuesta, así como los de verdadero y falso, etc.

7.2Creación de un cuestionario.

Como es un ejemplo de creación de un cuestionario haremos uno de prueba con preguntas simples y sin relación con la auditoría.

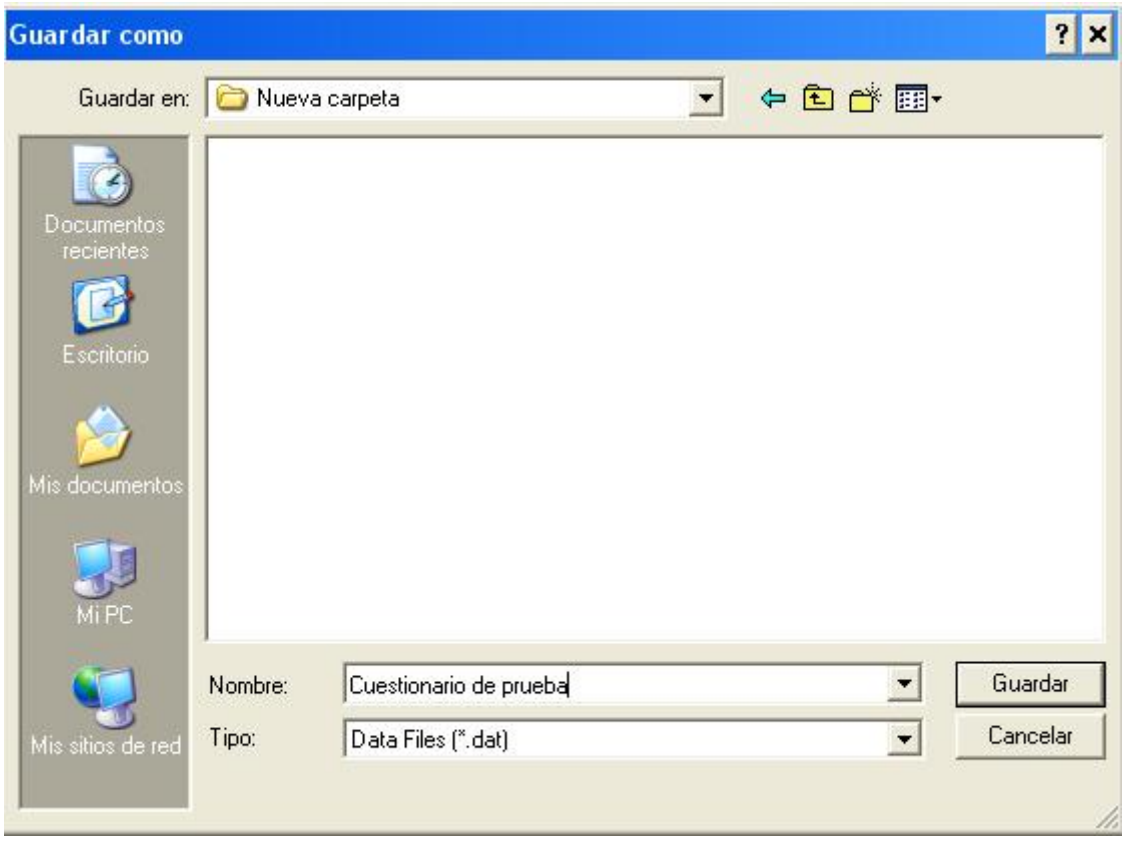
Empezaremos ejecutando el archivo el cual nos mostrará la siguiente imagen.



En la cual podemos desde cargar un cuestionario guardado anteriormente como realizar uno nuevo.

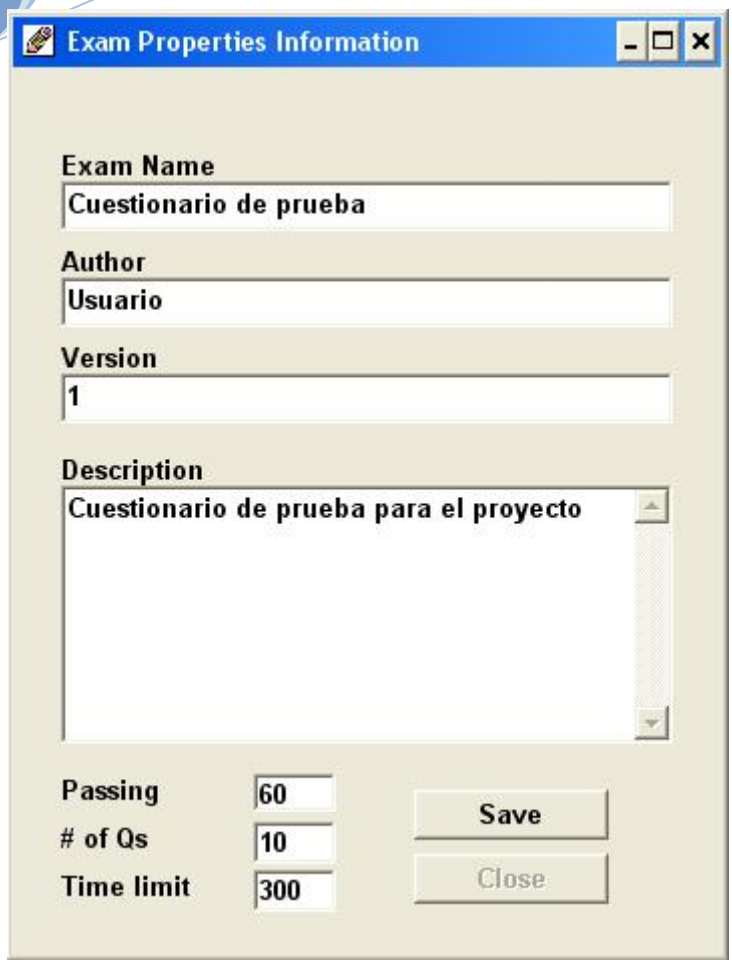
Ahora partiremos de uno nuevo

Si le damos al botón de crear (New) pasaremos a la siguiente imagen



En la cual pondremos un nombre al cuestionario para crearlo, así como la ubicación donde lo queremos guardar.

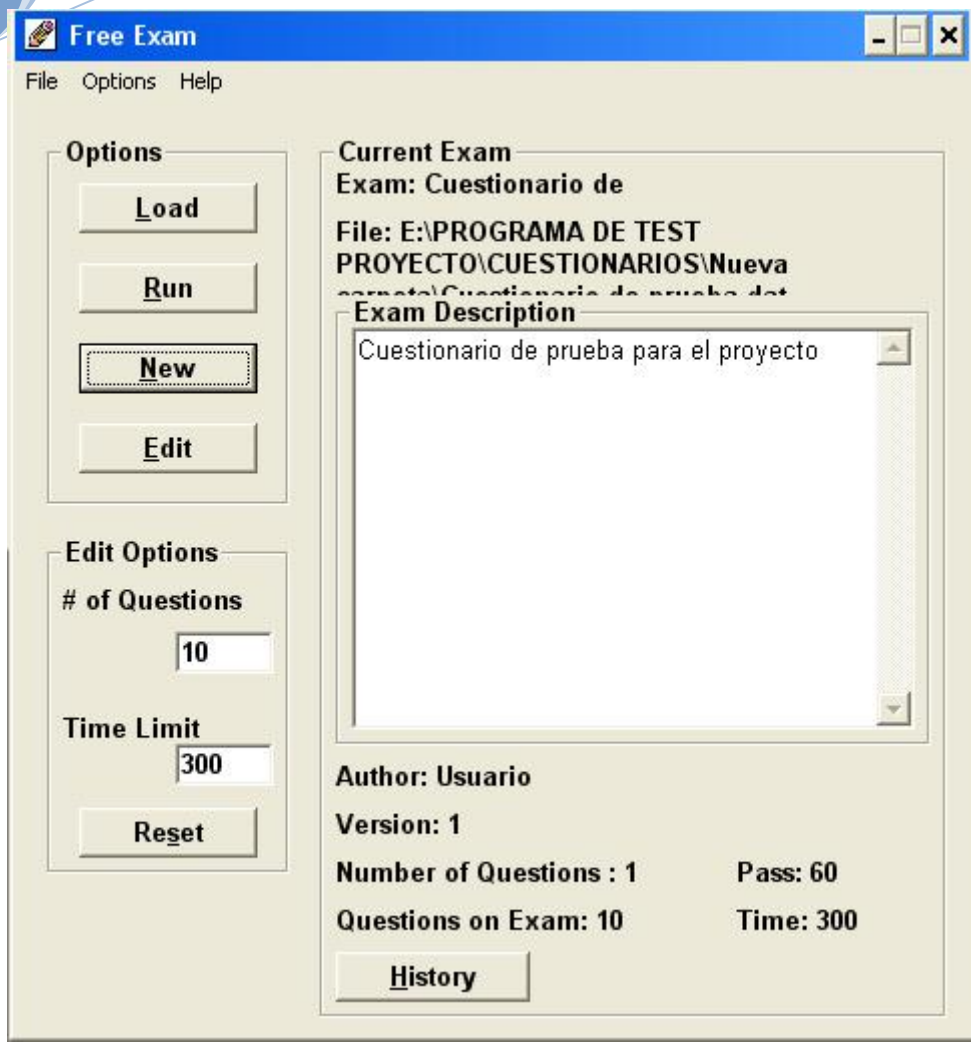
Una vez guardado pasaremos a la siguiente imagen.



En esta parte tendremos que poner un nombre al cuestionario, así como el autor que lo ha creado, su versión y una pequeña descripción para el proyecto.

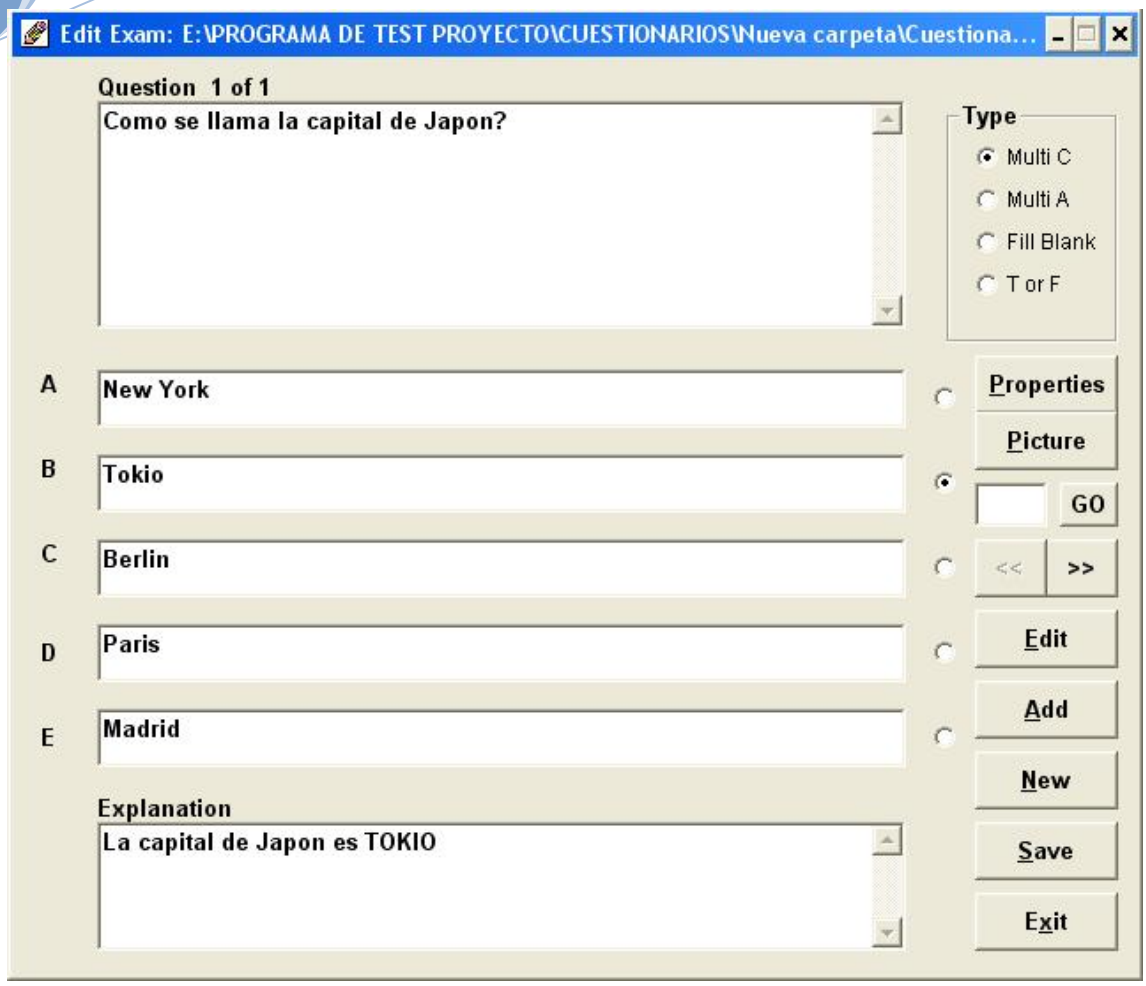
También tenemos que rellenar el tanto por ciento necesario que hay que tener acertado para que cuando se realice sea considerado como apto (en este caso 60%), así como el numero de cuestiones en este caso 10 y lo último sería el tiempo límite para hacerlo (como no hay necesidad de poner un tiempo límite simplemente ponemos la cantidad máxima de minutos para realizarlo, en este caso 300 minutos). Una vez cubiertas estas características le damos al botón de salvar (Save).

Ahora nos saldrá esta imagen:



En la cual nos comunica que el cuestionario ha sido creado y que será de 10 preguntas, sin embargo nos indica que solo hay 1 pregunta creada (el 1 viene por defecto), por lo tanto ahora hay que introducir las preguntas de nuestro cuestionario.

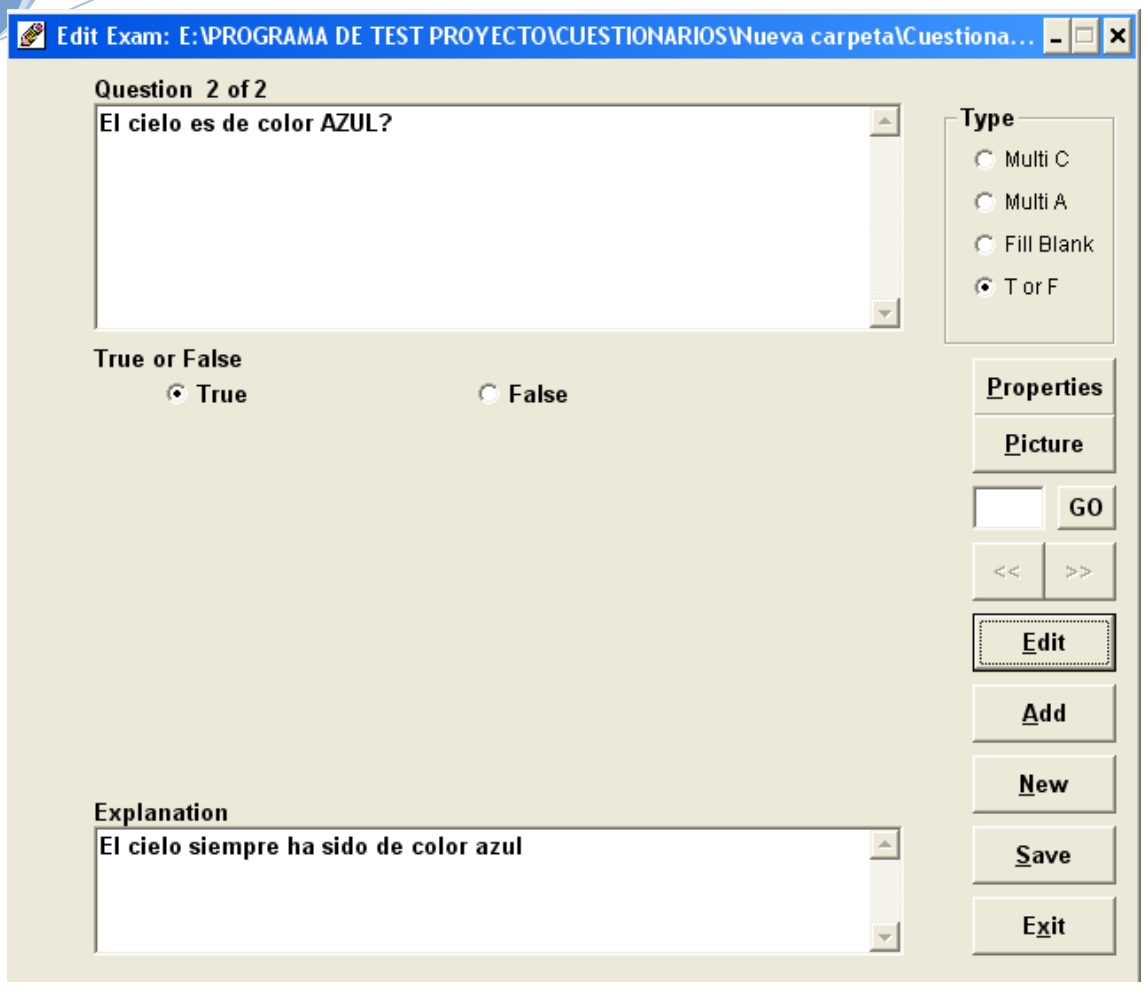
Para ello como ya tenemos seleccionado el cuestionario creado, por defecto, ahora tendremos que pulsar el botón de editar (Edit).



En este punto, tendremos que introducir la cuestión, así como sus posibles respuestas y la explicación. Para indicar cuál es la respuesta correcta haremos clic al lado de la pregunta en esta caso es la B.

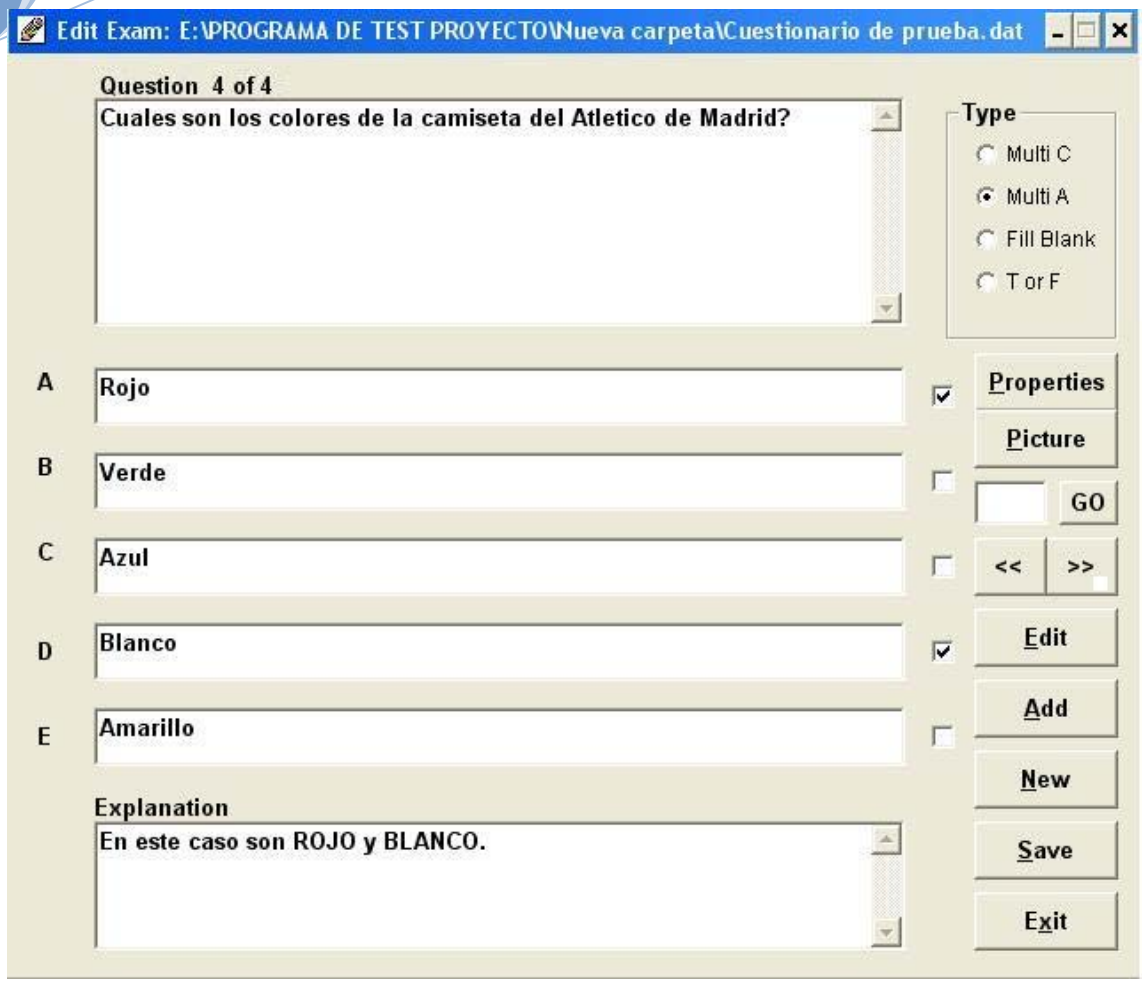
Una vez realizada correctamente la pregunta, como sus posibles respuestas y su explicación, haremos clic en el botón Edit, con lo que nos guardará pregunta en el test.

Para realizar la siguiente pregunta haremos clic en Add.



En esta segunda pregunta hemos elegido la opción de tipo VERDADERO o FALSO (true o false).

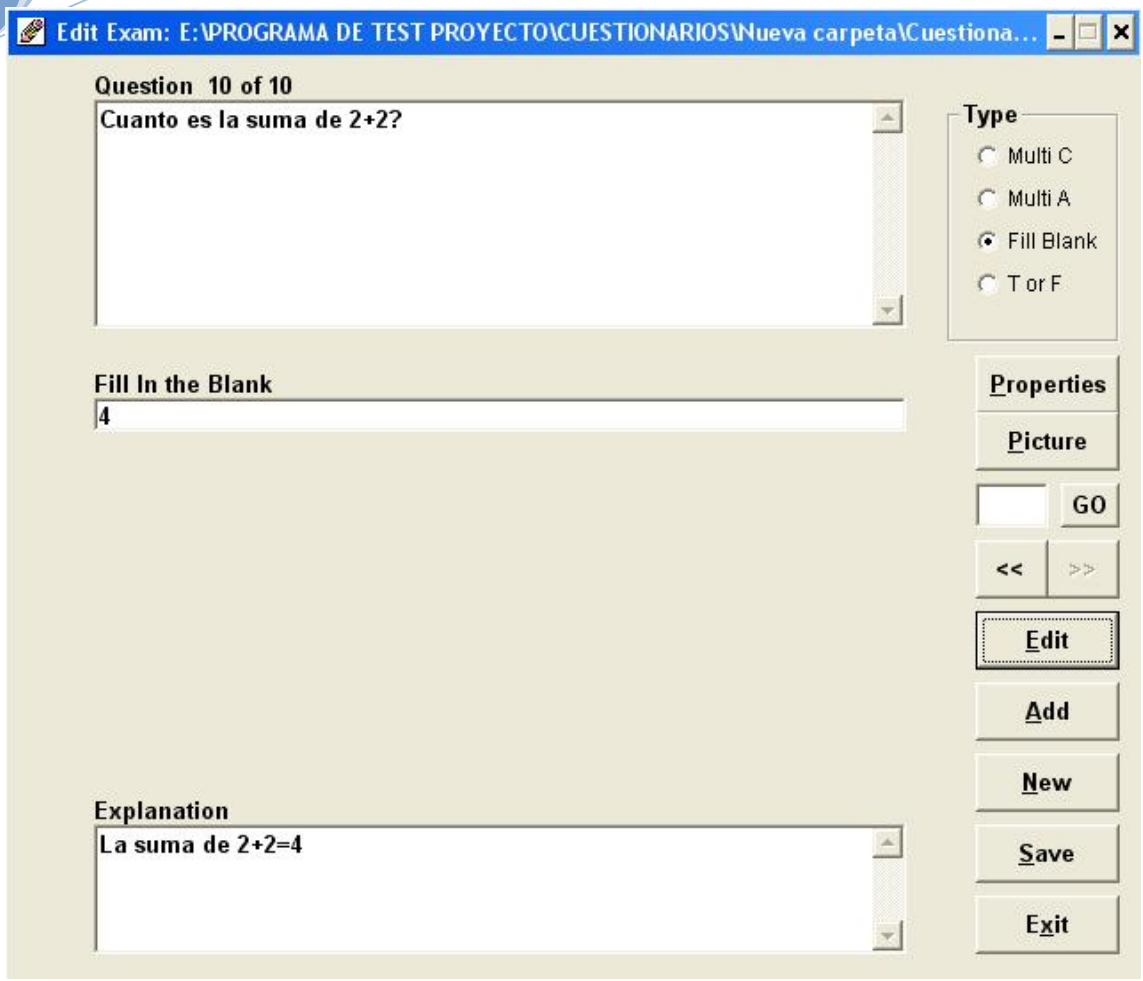
Al igual que la anterior rellenaremos los cuadros en blanco y volveremos a pulsar Edit para salvar la pregunta y Add para pasar a la siguiente.



En este caso hemos elegido una pregunta con multirespuesta.

Con botones en forma de flecha que hay encima del botón Edit, podremos movernos de una pregunta a otra y si escribimos el número de pregunta y luego pulsamos GO iremos directamente a esa pregunta.

Ahora haremos el último caso que podemos hacer de pregunta.

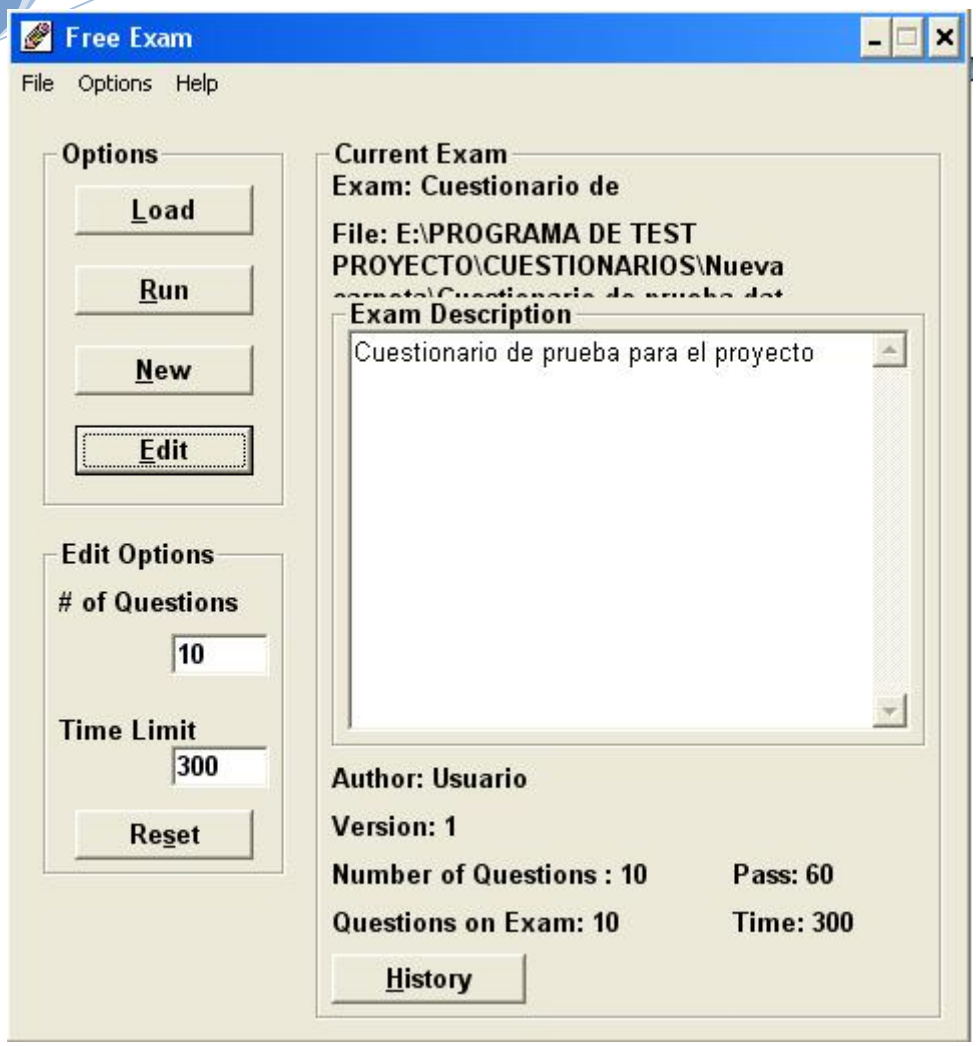


Esta pregunta consistirá en que hay que rellenar la respuesta.

Una vez finalizado nuestro cuestionario tendremos que pulsar el botón de Save con lo cual guardaremos de forma correcta nuestro cuestionario, para finalizar pulsaremos Exit.

En caso de que cuando realicemos el cuestionario por primera vez y aparezca una pregunta que no tiene nada que ver pulsaremos el botón de New. Para empezar a partir de cero.

Una vez pulsado el botón de Exit volveremos a aparecer en la siguiente figura

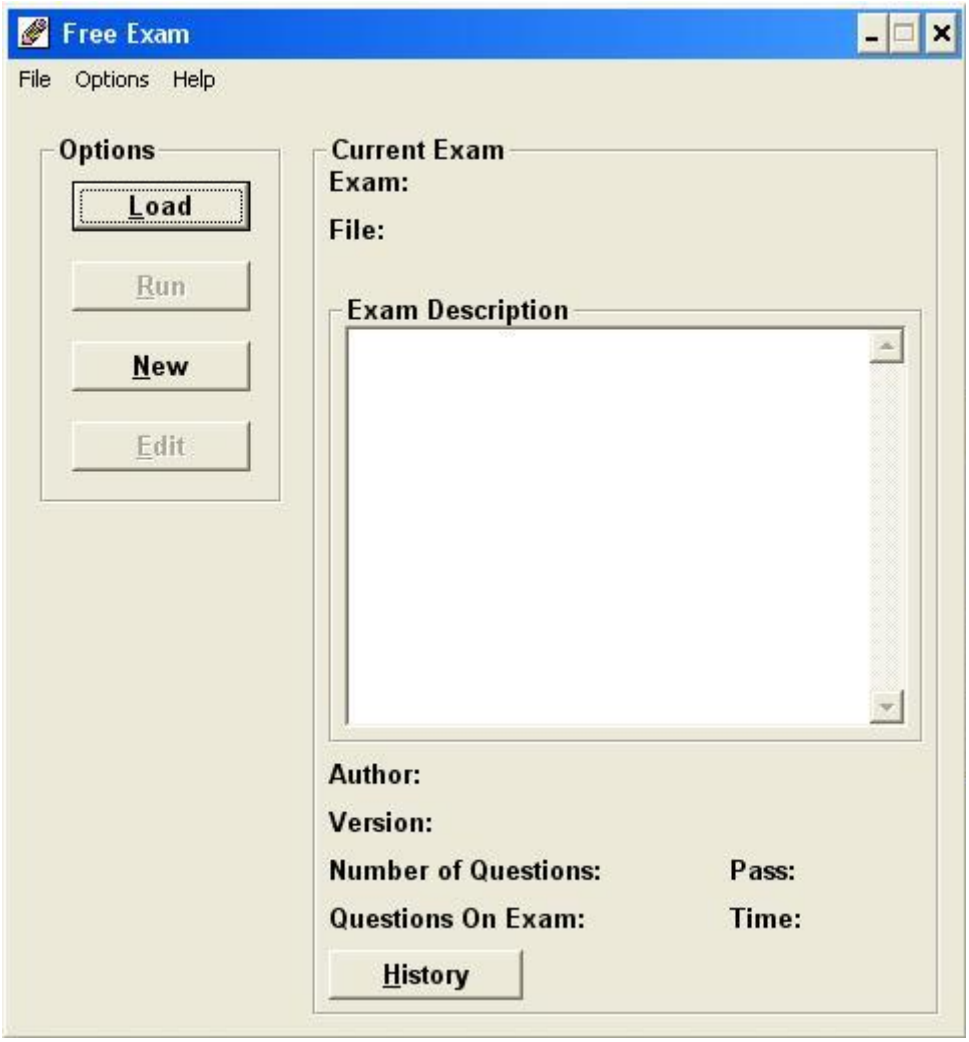


En la cual nos comunica que nuestro cuestionario de 10 preguntas tiene 10 preguntas creadas.

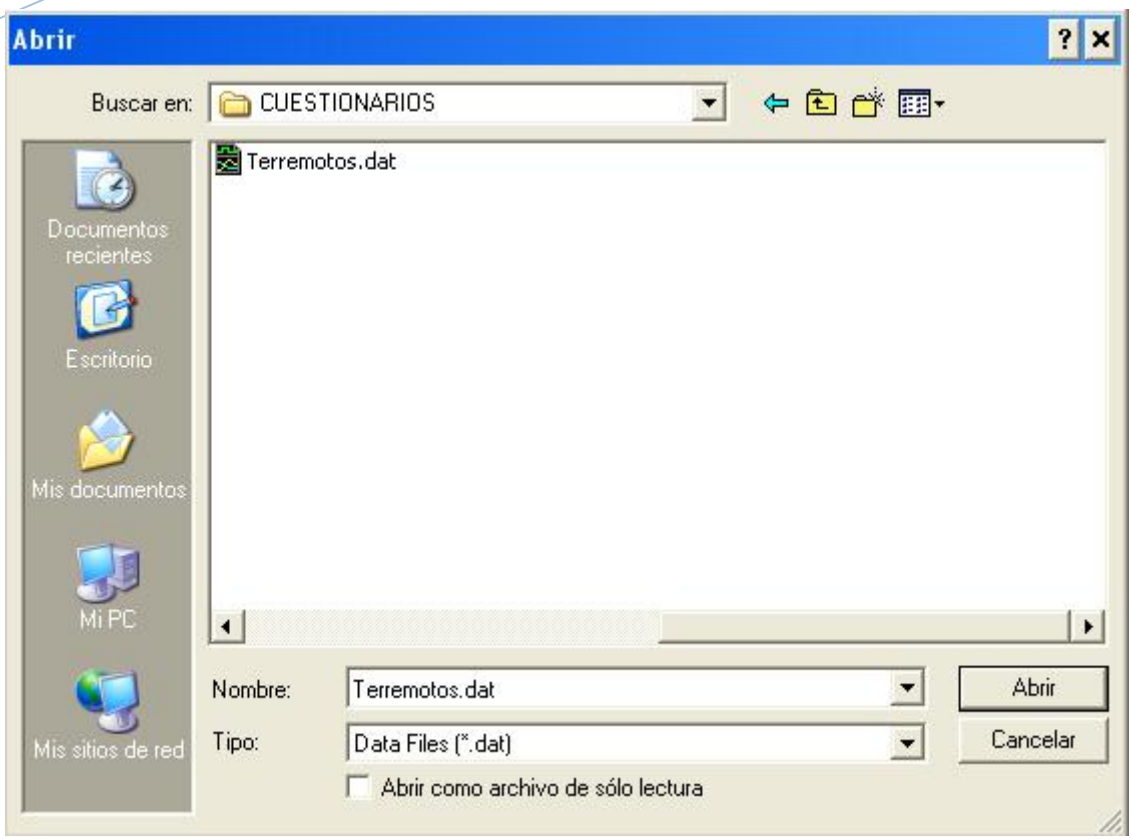
8.USO DEL CUESTIONARIO

En este punto comentaremos la realización de uno de los cuestionarios reales creados para el proyecto por parte del auditado. En este caso haremos el cuestionario sobre los terremotos.

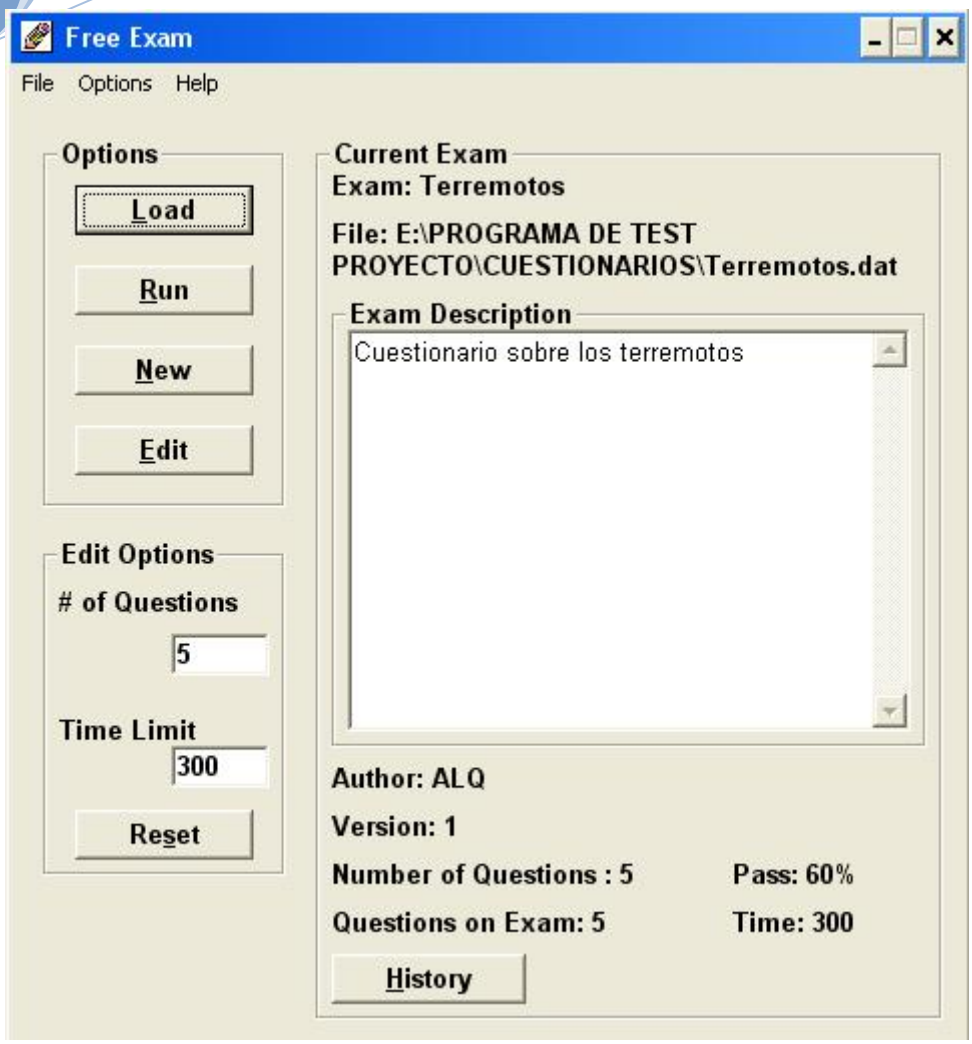
Ejecutamos el programa y empezaremos en esta ventana.



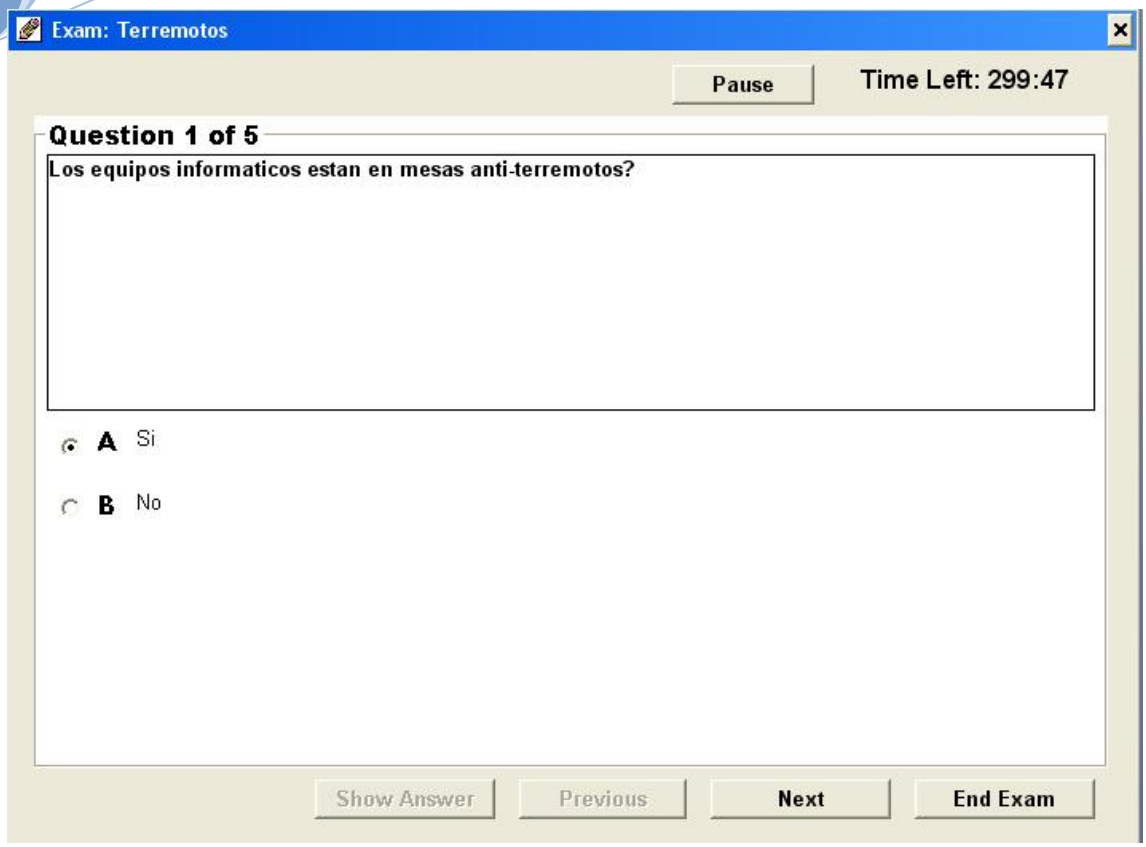
Ahora pulsaremos el botón de LOAD con el fin de cargar un cuestionario, el cual ya ha sido creado y almacenado.



En este caso elegimos el archivo Terremotos.dat el cual contiene el cuestionario a realizar.

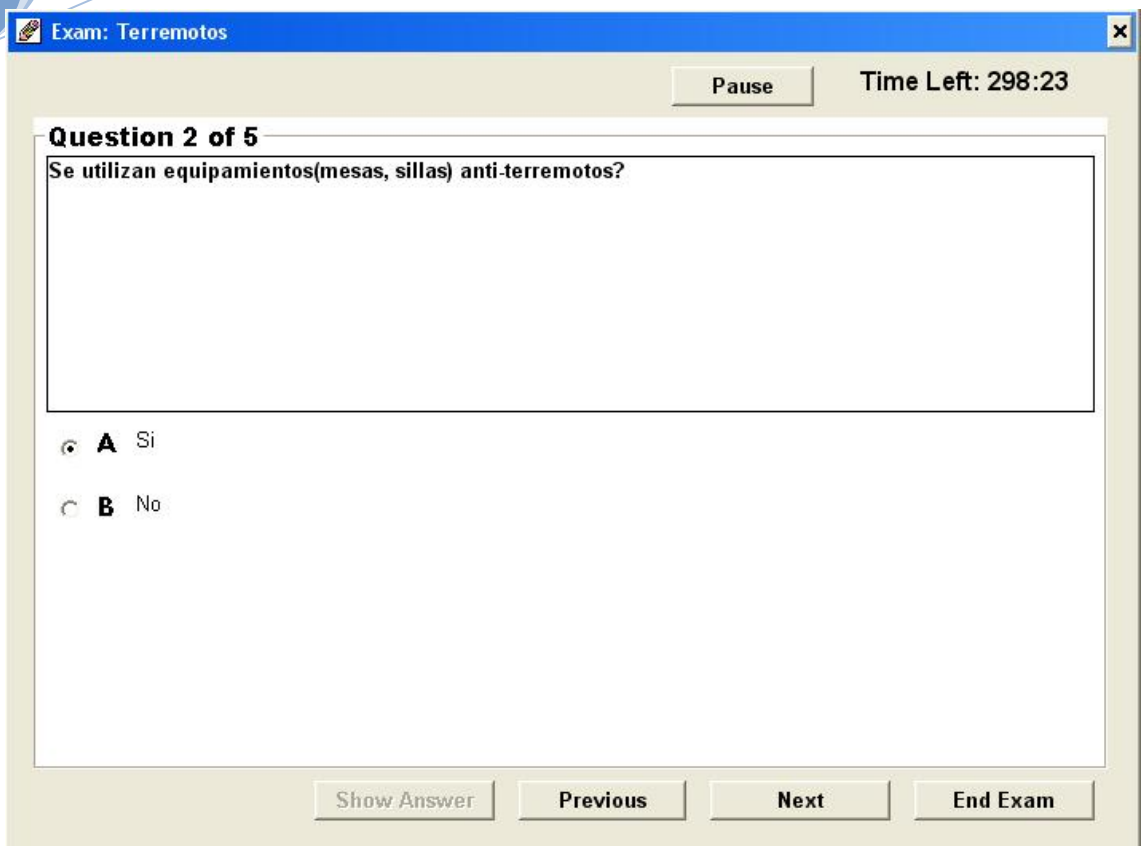


Ahora pulsaremos el botón de RUN para la realización del cuestionario

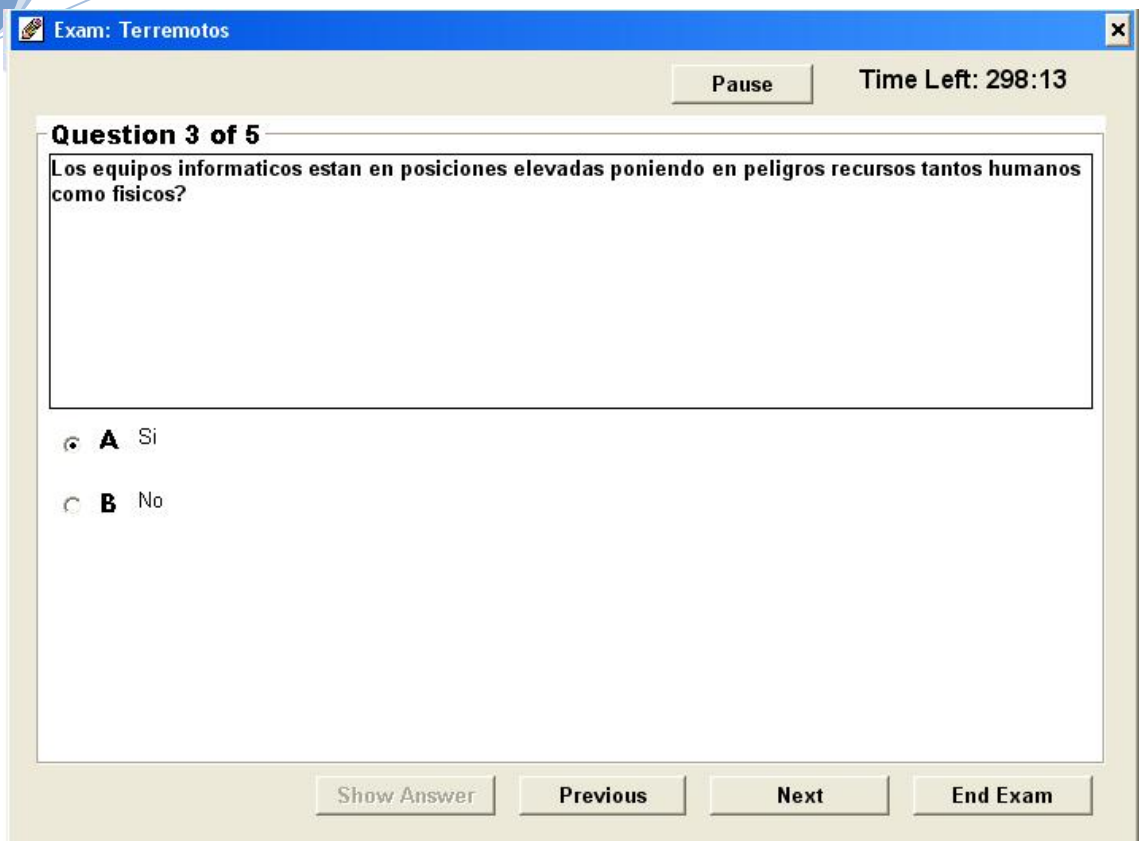


En este caso, tendremos que responder si nuestros equipos informáticos están en mesas anti-terremotos en nuestra entidad, dependiendo del auditado tendrá que elegir entre Sí o No.

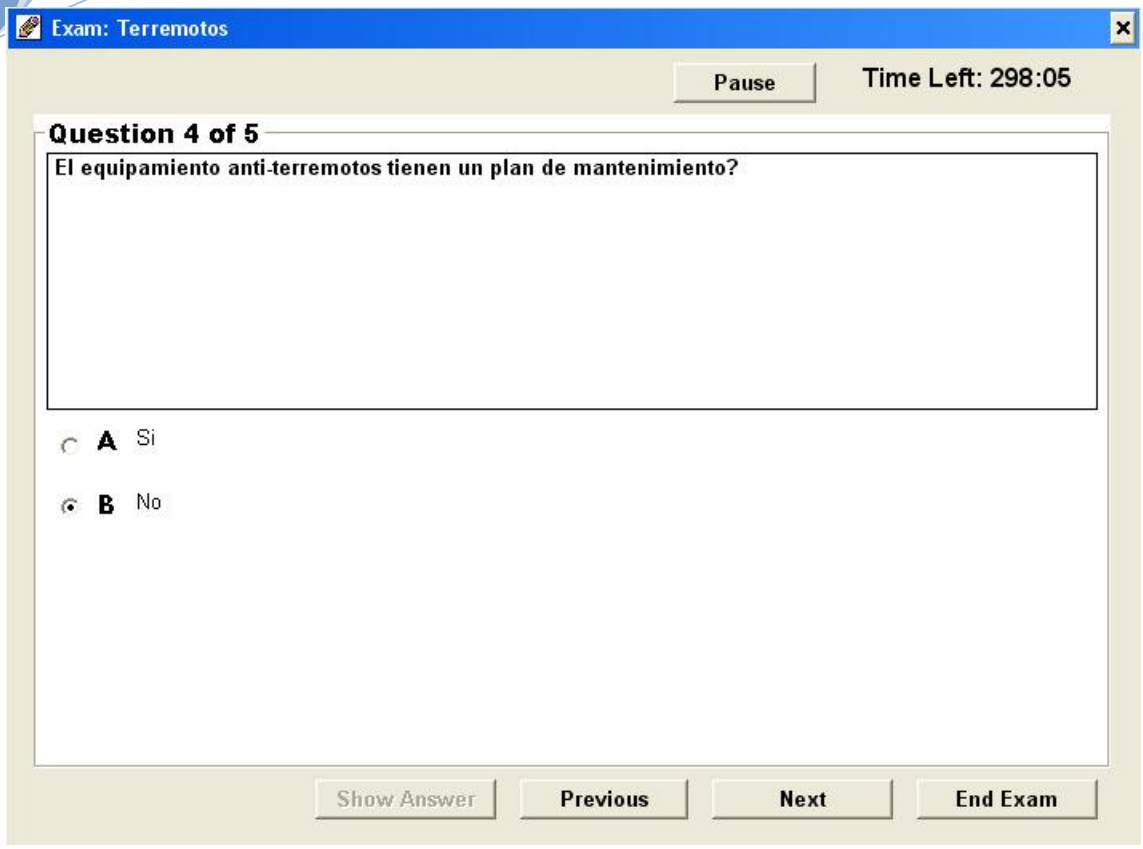
Una vez respondida dicha pregunta podemos dar al botón de NEXT para la siguiente pregunta del cuestionario.



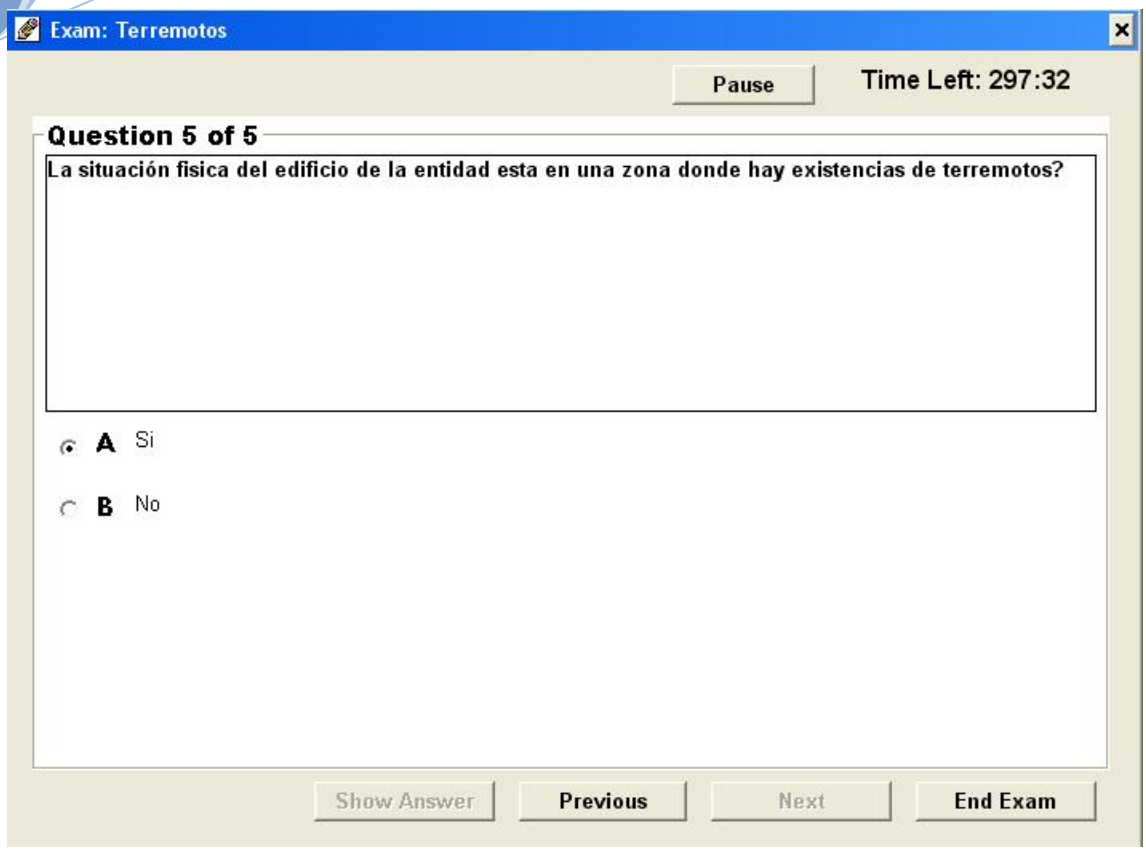
El botón de PREVIOUS nos hará movernos sobre las cuestiones anteriores por si queremos volver a leer y responder una pregunta, mientras que el NEXT nos moverá para adelante.



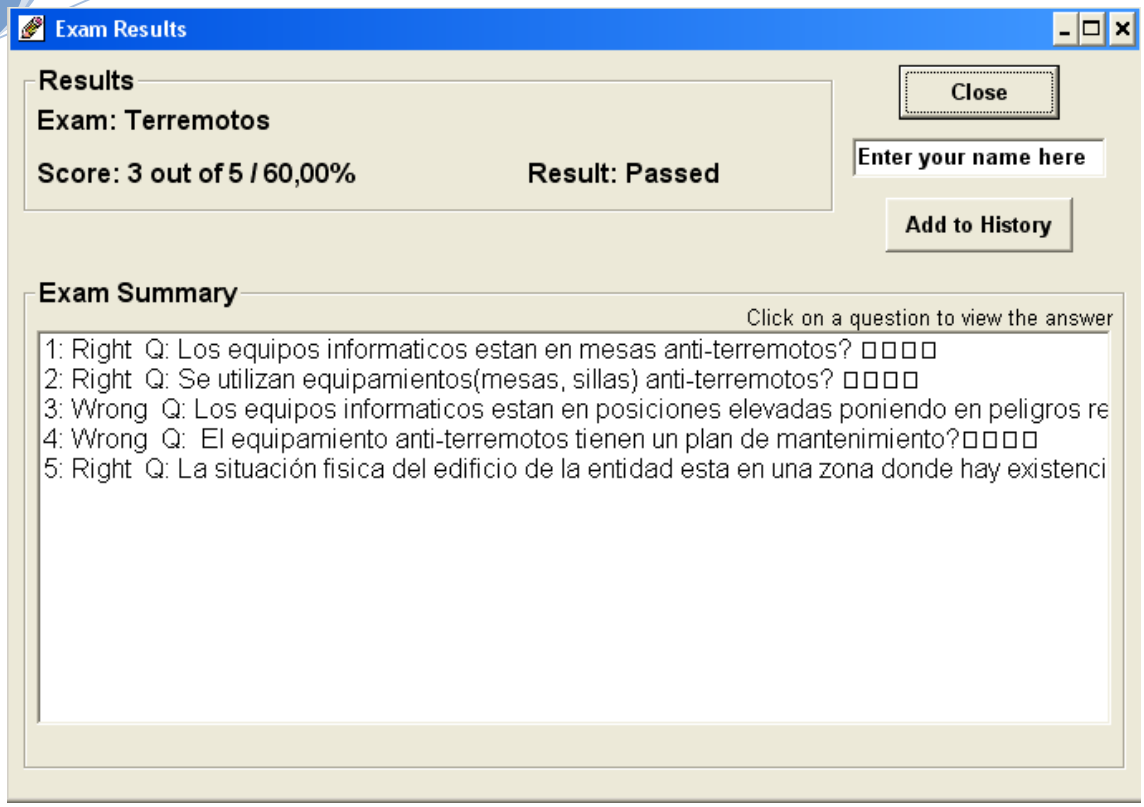
Contestamos y pasamos a la siguiente pregunta.



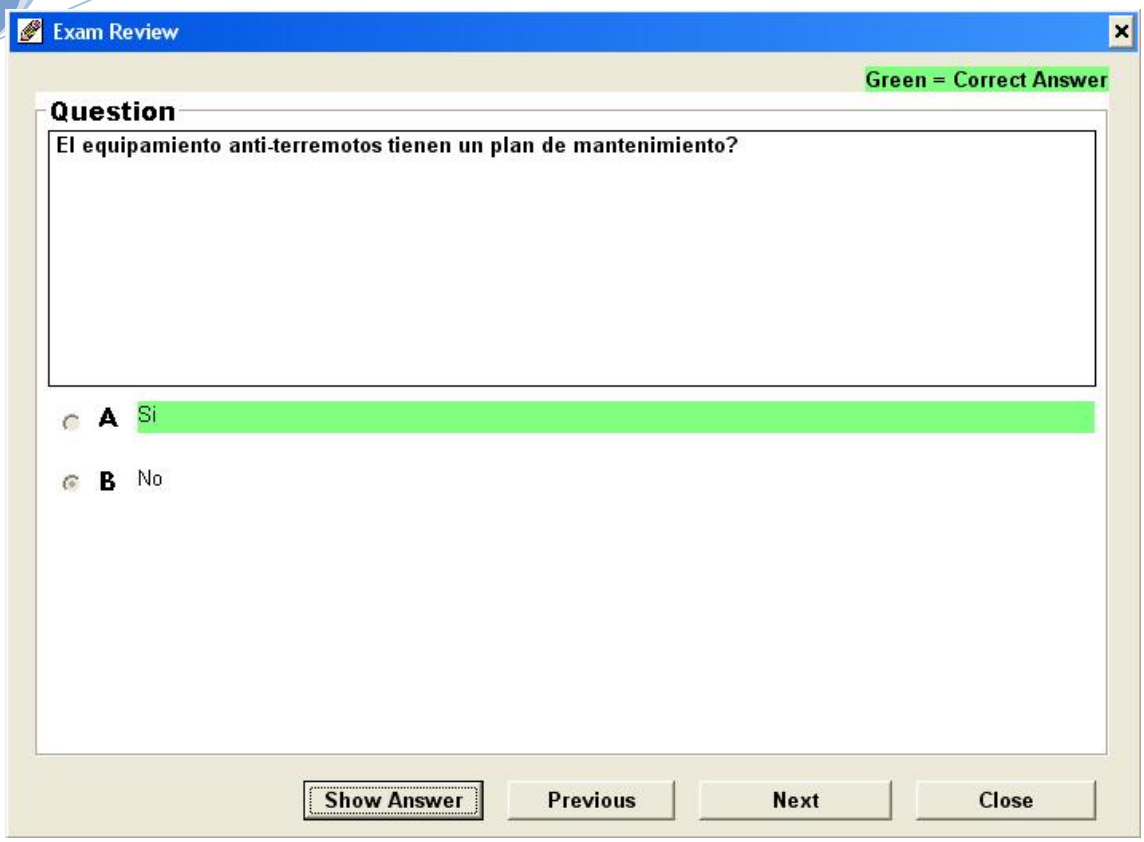
También en cualquier momento podemos parar de hacer el cuestionario pulsando el botón de PAUSE, pero en estos cuestionarios no es necesario debido a que tienen un tiempo bastante grande para realizarlos.



Una vez realizada la última pregunta del cuestionario, haremos clic en el botón END EXAM con el fin de que nos muestre los resultados obtenidos.

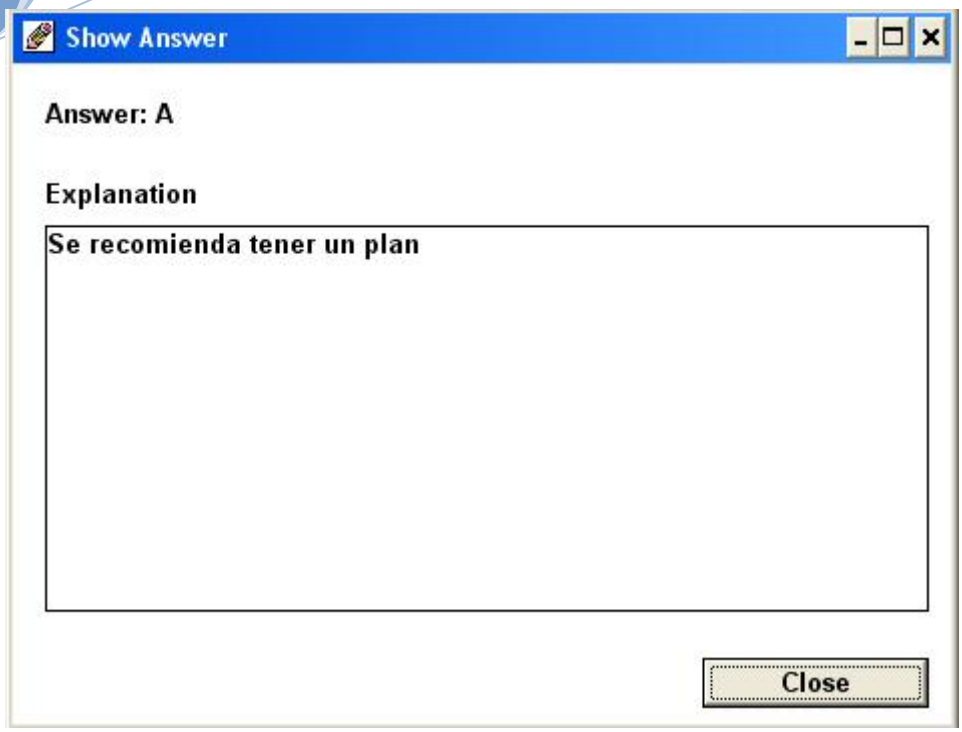


En esta imagen nos indica que ha sido apto, al tener un 60% y por tanto al ser igual o mayor (en este caso igual a la hora de tener un 60% como mínimo de cuestiones correctas) correcto de las cuestiones de la auditoría, además si hacemos clic en cualquier pregunta nos mostrará los siguiente.



Esta imagen nos muestra la pregunta seleccionada, así como la respuesta correcta en color verde (en este caso la A), y la respuesta del auditado (en ese caso la B), que tiene que ser para una entidad a la hora del equipamiento de los terremotos.

Para finalizar si pulsamos el botón SHOW ANSWER, nos mostrará una pequeña explicación.



En la explicación avisamos que se recomienda tener un plan de mantenimiento.

9.PREGUNTAS DEL CUESTIONARIO

9.1 Introducción

En este punto indicaremos todas las preguntas que he introducido en los cuestionarios realizados. Las preguntas se agrupan dependiendo del tipo de cuestionario.

Cabe recalcar que la mayoría de preguntas se responden con Sí o No, he pensado en la idea de realizarlos con múltiples pesos (nada, poco, bastante, mucho, todo, o usos de tantos por cientos), pero el problema que me surgía era el siguiente.

Un caso:

¿Tiene el mismo significado decir "poco" para el auditado de una gran empresa que para una pequeña?

Si un auditor estuviera realizando una auditoría y le preguntase al auditado ¿cuántos ordenadores sin control de acceso tiene en su organización? Y este respondiera al cuestionario con la respuesta de "pocos", ¿tendría el mismo significado si la entidad a la que estamos haciendo la auditoría fuese pequeña? Tal vez "pocos" para una entidad grande podría ser una grave brecha de seguridad, mientras que para una entidad pequeña sería una mínima brecha.

Otro caso:
¿Y si el auditado respondiera con un %?

Si el auditado comenta que solo tiene menos de un 10% de ordenadores sin control de acceso tal vez en una entidad pequeña que tiene unos 20-50 equipos informáticos, ese tanto por ciento sería mínimo, siendo de unos 2-5 ordenadores como mucho y siendo así una brecha fácil de solucionar, pero imaginemos que es una empresa multinacional con cientos o miles de ordenadores repartidos por todas sus oficinas, ese tanto por ciento aunque es mínimo tiene una cantidad altísima de equipos sin control de acceso, siendo una gravísima brecha de seguridad en sus equipos.

No se puede castigar o penalizar por igual a una entidad que sea grande, mediana o pequeña. Por tanto los pesos tendrían que ser diferentes para cada tipo de entidad.

Por estas razones he decidido que las cuestiones se respondan con un sí o no, es decir se cumple o no se cumple. Sí = 1 No = 0.

Además la decisión de hacerlo en base a dos únicas respuestas se centra en que el cuestionario puede aplicarse a cualquier tipo de tamaño de empresa tanto grande, mediana o baja.

Para que un cuestionario sea "apto" tendrá que tener como mínimo un 60% como para garantizar que tiene una seguridad mínima, aunque posiblemente no la suficiente, ya que por debajo de ese 60% el auditado tendría serios problemas, ante posibles incidencias en el futuro. Aun así será el auditor quien tomará la última palabra a la hora de elegir los tantos por cientos y de contemplar ciertos aspectos los cuales pueden escapar a los cuestionarios, al fin al cabo, el auditor tomará las respuestas de dichos cuestionarios como parte de sus informes a la hora de la realización de la auditoría, ya que sirve de apoyo al auditor.

Por último, tengo que comentar que se recomienda hacer los cuestionarios con respuestas basadas en múltiples pesos, pero para ello hay que conocer previamente el tamaño de la entidad para ajustar los pesos a sus correspondientes medidas para las determinadas entidades.

Preguntas.

A continuación pondremos todas las preguntas de los cuestionarios realizados.

9.2 Cuestiones

CUESTIONARIOS:

TERREMOTOS	
1. ¿La situación física del edificio de la entidad está en una zona donde hay existencias de terremotos?	Sí-No
2. ¿Los equipos informáticos están en posiciones elevadas poniendo en peligro recursos tantos humanos como físicos?	Sí-No
3. ¿Se utilizan equipamientos(mesas, sillas) anti-terremotos?	Sí-No
4. ¿Los equipos informáticos están en mesas anti-terremotos?	Sí-No
5. ¿El equipamiento anti-terremotos tienen un plan de mantenimiento?	Sí-No
INUNDACIONES	
1. ¿La situación física del edificio de la entidad está en una zona donde hay existencia de inundaciones?	Sí-No
2. ¿La situación física del edificio de la entidad está en una zona donde hay existencia de lagos, riachuelos, ríos, mar?	Sí-No
3. ¿Se ha establecido el uso de detectores de agua en el edificio de la entidad?	Sí-No
4. ¿Existencia de cañerías en mal estado?	Sí-No
5. ¿Se revisan las cañerías?	Sí-No
6. ¿Existencia de cañerías cerca de componentes eléctricos?	Sí-No
7. ¿Los detectores de agua tienen un plan de mantenimiento?	Sí-No
8. ¿Hay pulsador de alarma de inundación para ser pulsado por el personal de la entidad?	Sí-No
9. ¿Las alarmas de inundación avisan a los bomberos, hospitales, policía?	Sí-No
FUEGOS	
1. ¿El personal de la entidad fuma dentro de las instalaciones de la entidad?	Sí-No
2. ¿Se han establecido zona de fumadores para el personal de la entidad con el fin de evitar de que fumen a escondidas dentro del edificio(baños, escaleras)?	Sí-No
3. ¿Hay paneles eléctricos deteriorados?	Sí-No
4. ¿Hay simulacros de incendios?	Sí-No
5. ¿Uso de material inflamable(mesas, sofas,etc)?	Sí-No
6. ¿Hacen cursos de formación de primeros auxilios por parte del personal de la entidad?	Sí-No
7. ¿Hacen cursos de formación contra incendios por parte del personal de la entidad?	Sí-No
8. ¿Existen almacenamiento de papel en grandes proporciones?	Sí-No
9. ¿Existen extintores dentro de la entidad?	Sí-No

10. ¿Existen indicaciones de la situación de los extintores de la entidad?	Sí-No
11. ¿Existen indicaciones sobre donde está la puerta de salida?	Sí-No
12. ¿Hay detectores de fuego y humo en la entidad?	Sí-No
13. ¿Hay pulsador de alarma de fuego para ser pulsado por el personal de la entidad?	Sí-No
14. ¿Existen indicaciones sobre donde está el pulsador de alarma?	Sí-No
15. ¿Las alarmas avisan a los bomberos, hospitales, policía?	Sí-No
16. ¿Los detectores tienen un plan de mantenimiento?	Sí-No
17. ¿Los extintores tienen un plan de mantenimiento?	Sí-No
18. ¿Los cables eléctricos están dentro de paneles?	Sí-No
19. ¿Tienen los servidores protección automática contra el fuego?	Sí-No
BACK-UPS(información salvaguardada)	
1. ¿Existencias de Back-ups?	Sí-No
2. ¿La información se guarda en los back-ups de forma periódicas?	Sí-No
3. ¿Todas las copias de la información se guardan junta?	Sí-No
4. ¿Los Back-ups están en una situación física segura(lejos de la entidad) en caso de fuegos, inundaciones, etc.?	Sí-No
5. ¿Los back-ups están protegidos ante robos(uso de salas de seguridad, cajas fuertes)?	Sí-No
6. ¿Los Back-ups tienen un plan de mantenimiento?	Sí-No
7. ¿Los back-ups están protegidos ante ataques informáticos(hackers, virus, crackers,etc)?	Sí-No
8. ¿Existen procedimientos para la reconstrucción de los archivos en caso de su destrucción?	Sí-No
9. ¿Están identificados los archivos con información clasificada?	Sí-No
10. ¿Dicha información clasificada tiene clave de acceso?	Sí-No
11. ¿Hay certificación de que los archivos borrados?	Sí-No
12. ¿Hay personal autorizado para firmar la salida de los archivos clasificados?	Sí-No
13. ¿Hay responsable en caso de fallo de los backups?	Sí-No
TORMENTAS ELECTRICAS Y PICOS DE TENSION - ELECTRICIDAD	
1. ¿ La situación física del edificio de la entidad está en una zona donde hay existencia de tormentas eléctricas?	Sí-No
2. ¿Existe la instalación de pararrayo en el edificio de la entidad?	Sí-No
3. ¿Las tormentas eléctricas han producido daños en lo equipos informáticos en forma física? (Placas quemadas, ordenadores inutilizados completamente)	Sí-No
4. ¿Las tormentas eléctricas han producido perdida de la información(bases de datos dañadas) en los equipos informáticos?	Sí-No
5. ¿Los pararrayos tienen un plan de mantenimiento?	Sí-No
6. ¿Existen SAI (sistemas de alimentación ininterrumpida)?	Sí-No
7. ¿Existe un plan de mantenimiento de los SAI?	Sí-No

8. ¿Existe sobrecarga de corriente eléctricas?	Sí-No
9. ¿Existe un plan de mantenimiento de los paneles eléctricos?	Sí-No
CONTROL DE ACCESO A LAS INSTALACIONES- SEGURIDAD FISICA	
1. ¿Uso de cámaras de seguridad?	Sí-No
2. ¿Sistemas de sensores de movimiento?	Sí-No
3. ¿Las puertas están cerradas?	Sí-No
4. ¿Uso de sistemas de control de acceso a las salas(tarjetas, biometría, etc.)?	Sí-No
5. ¿Existencia de personal de seguridad?	Sí-No
6. ¿Existencia de un registro de entrada al edificio?	Sí-No
7. ¿Existencia de un registro de salida del edificio?	Sí-No
8. ¿Existencia de un registro de entrada de las salas del edificio?	Sí-No
9. ¿Existencia de un registro de salida de las salas del edificio?	Sí-No
10. ¿Las cámaras de seguridad están bien colocadas?	Sí-No
11. ¿Los sensores de movimiento están bien colocados?	Sí-No
12. ¿Existe un plan de mantenimiento de las cámaras de seguridad?	Sí-No
13. ¿Existe un plan de mantenimiento de los sensores de movimiento?	Sí-No
14. ¿Existe un plan de mantenimiento de los sistemas de control de acceso a las salas?	Sí-No
15. ¿Existencia de un registro para el edificio para invitados(personas que no trabajan en la entidad)?	Sí-No
16. ¿Son capaces de acceder personas no relacionadas con la entidad en el edificio?	Sí-No
17. ¿Se hacen pruebas de personas colándose en el edificio para comprobar las medidas?	Sí-No
18. ¿El personal de seguridad está bien formado?	Sí-No
19. ¿Existencia de cursos de reciclaje para el personal de seguridad?	Sí-No
20. ¿Tras finalizar la jornada laboral se cierran las puertas?	Sí-No
21. ¿El personal de la entidad respeta ese control?	Sí-No
22. ¿El trato del personal de seguridad es correcto?	Sí-No
23. ¿Existe división de la responsabilidad para tener un control mejor de la seguridad?	Sí-No
24. ¿Se investiga a los vigilantes antes de ser contratados?	Sí-No
25. ¿Se bloquean las tomas de red que no son utilizadas para evitar pinchazos de terceras personas?	Sí-No
26. ¿Una vez despedido un empleado se le retira su tarjeta de acceso a la entidad?	Sí-No
CONTROL DE ACCESO A LOS EQUIPOS INFORMATICOS	
1. ¿Uso de contraseñas por parte de los empleados?	Sí-No
2. ¿Las contraseñas tienen más de 8 caracteres?	Sí-No
3. ¿La contraseña es alfanumérica?	Sí-No

4. ¿Existen diferentes niveles de acceso?(ejecutivos, programadores, analistas)	Sí-No
5. ¿Se registra la entrada al equipo informático?	Sí-No
6. ¿Se registra la salida al equipo informático?	Sí-No
7. ¿Los empleados son informados sobre los riesgos de las contraseñas?	Sí-No
8. ¿Uso de contraseñas que no tienen nada que ver con información del personal de la entidad(nombre, teléfono, matrícula del coche?	Sí-No
9. ¿Las cuentas de los empleados que vayan a ser despedidos son bloqueadas o capadas antes del aviso de despido?	Sí-No
10. ¿Las contraseñas son cambiadas periódicamente?	Sí-No
11. ¿Las contraseñas de cada empleado son diferentes para cada tipo de acceso?	Sí-No
12. ¿Se comprueba que las cuentas que están en desuso son eliminadas?	Sí-No
13. ¿Existe un responsable del control de dichas cuentas?	Sí-No
14. ¿Hay diferentes modalidades de accesos dependiendo del grado de acceso del empleado?(lectura, escritura, borrado, ejecución)	Sí-No
15. ¿El empleado solo puede acceder a los recursos en determinadas horas del día?	Sí-No
16. ¿El empleado solo puede acceder a determinados equipos informáticos?	Sí-No
17. ¿Se cambian las contraseñas que vienen por defecto en los equipos informáticos?	Sí-No
18. ¿Existen cuentas sin contraseña?	Sí-No
19. ¿Existe un número limitado de intentos a la hora de introducir la contraseña?	Sí-No
SEGURIDAD LOGICA	
1. ¿Hay caída de la conexión a internet?	Sí-No
2. ¿Los equipos informáticos tienen los programas necesarios para trabajar?	Sí-No
3. ¿Son adecuadas las restricciones de la configuración del equipo?	Sí-No
4. ¿Se controla a los analistas?	Sí-No
5. ¿Se controla a los programadores?	Sí-No
6. ¿Existe un proceso de emergencia con el fin de que la información pueda llegar hasta el destinatario?	Sí-No
7. ¿Se comprueba que la información llegada al destinario es la misma que fue enviada desde el origen?	Sí-No
8. ¿La información transferida llega a ser recibida por terceros?	Sí-No
9. ¿Existen diferentes caminos de transmisión entre diferentes puntos?	Sí-No
METRICA	
1. ¿Se sabe la calidad del producto o servicio que realiza la entidad?	Sí-No
2. ¿Los empleados están realizando el producto o servicio de forma correcta?	Sí-No
3. ¿Los empleados están realizando el producto o servicio de forma eficaz?	Sí-No
4. ¿Los empleados están realizando el producto o servicio de forma rápida?	Sí-No

5. ¿Se conocen los beneficios de los nuevos procesos?	Sí-No
6. ¿Se conocen los beneficios de las herramientas utilizadas?	Sí-No
7. ¿Se conocen los beneficios de los métodos utilizados?	Sí-No
8. ¿La métrica indirecta es?	
- Centrada en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, etc.	Sí-No
- Engloba la velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, etc.	Sí-No
9. ¿La métrica directa es?	
- Centrada en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, etc.	TRUE - FALSE
- Engloba la velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, etc.	TRUE - FALSE
10. ¿La medida…?	
- Nos proporciona una indicación cuantitativa de cantidad, dimensiones, capacidad, tamaño y extensión de algunos de los atributos de un producto o de su proceso.	TRUE - FALSE
- Proceso por el cual los números son asignados a atributos o entidades en el mundo real tal como son definidos de acuerdo a las reglas claramente definidas.	TRUE - FALSE
11. ¿La medición?	
- Nos proporciona una indicación cuantitativa de cantidad, dimensiones, capacidad, tamaño y extensión de algunos de los atributos de un producto o de su proceso.	TRUE - FALSE
- Proceso por el cual los números son asignados a atributos o entidades en el mundo real tal como son definidos de acuerdo a las reglas claramente definidas.	TRUE - FALSE
12. ¿Las métricas son ambiguas?	Sí-No
13. ¿Uso de estadísticas?	Sí-No
14. ¿Automatización de la recogida de datos?	Sí-No
15. ¿Cual es el orden de las etapas del proceso de medición?	
-Colección, análisis, formulación, realimentación e interpretación.	TRUE - FALSE
-Análisis, interpretación, realimentación, formulación y colección.	TRUE - FALSE

-Formulación, colección, análisis, interpretación y realimentación.	TRUE - FALSE
16. ¿Se utilizán métricas para evaluar a particulares?	Sí-No
17. ¿Existe incompatibilidad de métricas?	Sí-No
18. ¿Las métricas son fáciles de obtener?	Sí-No
19. ¿Las métricas están expresadas en porcentajes o en escala?	Sí-No
20. ¿Las métricas son detalladas?	Sí-No
21. ¿Con las métricas obtenemos los puntos débiles de nuestra entidad?	Sí-No
PREPARACION PARA LA IMPLEMENTACION DE LAS NORMATIVAS EN UNA ENTIDAD	
1. ¿Existe un mínimo de procesos definidos?	Sí-No
2. ¿Existe un compromiso por parte de todos los actores de la empresa?	Sí-No
3. ¿El ambiente laboral es agradable, sano y activo?	Sí-No
4. ¿El personal es consciente con la necesidad de mejoramiento?	Sí-No
5. ¿Existe una orientación hacia el trabajo en equipo de forma eficaz?	Sí-No
6. ¿Existe un plan y visión de futuro?	Sí-No
7. ¿Los objetivos están bien definidos?	Sí-No
8. ¿Existe apoyo entre los empleados?	Sí-No
9. ¿Existe comunicación entre los empleados?	Sí-No
10. ¿Hay una buena integración del trabajo entre los diferentes departamentos?	Sí-No
11. ¿Existe un sistema que refleje los objetivos conseguidos a lo largo del trabajo?	Sí-No
12. ¿Hay explotación del trabajador?	Sí-No
13. ¿Se desea la evolución de la entidad?	Sí-No
14. ¿La entidad va en busca de los clientes a través de técnicas comerciales?	Sí-No
15. ¿La entidad se centra en la efectividad y productividad en el mercado?	Sí-No
16. ¿Los planes concretos que tiene la entidad son ejecutados y medidos?	Sí-No
17. ¿Las ideas que surjan son expresadas libremente?	Sí-No
18. ¿Existe participación del empleado en la entidad?	Sí-No
19. ¿Se estimula al empleado a través de metas/resultados?	Sí-No
20. ¿Hay reuniones entre empleados y directivos?	Sí-No
21. ¿Existencia de una organización centrada hacia el servicio a clientes?	Sí-No
22. ¿La entidad está centrada en la búsqueda de evitar el trabajo individual?	Sí-No
23. ¿La entidad está centrada en la búsqueda de estudiar, conocer y comprender a la competencia?	Sí-No
24. ¿La entidad está centrada a la búsqueda del uso del Benchamarking?	Sí-No
CON LA NORMATIVA INSTALADA	

1. ¿Se ha dado de lado el uso de un sistema participativo?	Sí-No
2. ¿Se ha dado de lado el uso del just-in-time?	Sí-No
3. ¿Se ha dado de lado la seguridad en la entidad?	Sí-No
4. ¿Se ha dado de lado el uso de la participación de la administración?	Sí-No
5. ¿Se ha dado de lado el uso de la mejora continua?	Sí-No
6. ¿Se ha puesto un ritmo de trabajo a la entidad y a sus empleados el cual no es el suyo propio debido a la normativa?	Sí-No
7. ¿Los trabajadores son informados de lo que ocurre en la empresa?	Sí-No
8. ¿En el comité de calidad de la empresa existen representante de los trabajadores?	Sí-No
9. ¿Se motiva a los empleados con la normativa?	Sí-No
10. ¿La implantación de la norma se ha realizado por imposición y de malas maneras?(ejemplo, es lo que hay y vamos hacerlo)	Sí-No
11. ¿La normativa ha sido aplicada porque está de moda?	Sí-No
NORMATIVA ISO/IEC 27004 – Parte 1	
1. ¿La entidad tenía incorporado el modelo PDCA(plan-do-check-act)?	Sí-No
2. Con este modelo PDCA(plan-do-check-act) ¿se cumple el objetivo de indicar y avisar los valores de seguridad de la entidad?	Sí-No
3. Con este modelo PDCA(plan-do-check-act) ¿se cumple el objetivo de realizar una evaluación de la eficiencia del sistema de gestión de seguridad de la información?	Sí-No
4. Con este modelo PDCA(plan-do-check-act) ¿se cumple el objetivo de incluir niveles de seguridad que sirvan de guía para las revisiones del sistema de gestión de seguridad de la información?	Sí-No
5. Con este modelo PDCA(plan-do-check-act) ¿se cumple el objetivo de realizar una evaluación de la efectividad de la implementación de los controles de la seguridad de la entidad?	Sí-No
6. ¿El programa de medición está basado en un modelo de mediciones para la seguridad de la información?	Sí-No
7. ¿El modelo se centra en una arquitectura que relaciona los atributos medibles con una entidad relevante?	Sí-No
8. ¿Están definidos los atributos más importantes?	Sí-No
9. ¿Existe frecuencia en cada medición?	Sí-No
10. ¿Para realizar el establecimiento y la operación del programa de medición se definen los procesos?	Sí-No
11. ¿Para realizar el establecimiento y la operación del programa de medición se desarrollan las mediciones?	Sí-No
12. ¿Para realizar el establecimiento y la operación del programa de medición se implementa el programa?	Sí-No
13. ¿Para realizar el establecimiento y la operación del programa de medición se revisan las mediciones?	Sí-No
14. ¿Las mediciones son cuantitativas?	Sí-No
15. ¿Las mediciones son indivisibles?	Sí-No

16. ¿Las mediciones están bien definidas?	Sí-No
17. ¿Las mediciones son razonables?	Sí-No
18. ¿A la hora de seleccionar los controles necesarios la entidad define el programa?	Sí-No
19. ¿A la hora de seleccionar los controles necesarios define sus respectivos indicadores?	Sí-No
20. ¿En el modelo PDCA(plan-do-check-act) en qué consiste el "PLAN"?	
-Revisión y mejora de las métricas de seguridad.	TRUE - FALSE
-Adaptar procedimientos y controles para la obtención de datos.	TRUE - FALSE
-Definir las métricas y establecer el sistema de gestión de seguridad de la información(SGSI)	TRUE - FALSE
-Revisión de los datos obtenidos de las métricas realizadas.	TRUE - FALSE
21. ¿En el modelo PDCA(plan-do-check-act) en qué consiste el "DO"?	
-Revisión y mejora de las métricas de seguridad.	TRUE - FALSE
-Adaptar procedimientos y controles para la obtención de datos.	TRUE - FALSE
-Definir las métricas y establecer el sistema de gestión de seguridad de la información(SGSI)	TRUE - FALSE
-Revisión de los datos obtenidos de las métricas realizadas.	TRUE - FALSE
22. ¿En el modelo PDCA(plan-do-check-act) en qué consiste el "CHECK"?	
-Revisión y mejora de las métricas de seguridad.	TRUE - FALSE
-Adaptar procedimientos y controles para la obtención de datos.	TRUE - FALSE
-Definir las métricas y establecer el sistema de gestión de seguridad de la información(SGSI)	TRUE - FALSE
-Revisión de los datos obtenidos de las métricas realizadas.	TRUE

	- FALSE
23. ¿En el modelo PDCA(plan-do-check-act) en qué consiste el "ACT"?	
-Revisión y mejora de las métricas de seguridad.	TRUE - FALSE
-Adaptar procedimientos y controles para la obtención de datos.	TRUE - FALSE
-Definir las métricas y establecer el sistema de gestión de seguridad de la información(SGSI)	TRUE - FALSE
-Revisión de los datos obtenidos de las métricas realizadas.	TRUE - FALSE
24. ¿Para la implementación de un cuadro de mando, la entidad señala toda la información que sea totalmente necesaria de una forma correcta?(resumida, entendible, sencilla, etc)	Sí-No
25. ¿Para la implementación de un cuadro de mando, la entidad resume la representación usando un juego de colores el cual nos sirva para indicar los cambios de estado?	Sí-No
26. ¿Para la implementación de un cuadro de mando, la entidad tiene el apoyo de la dirección?	Sí-No
27. ¿En relación con la dirección, se comunica de inmediato cualquier tipo de acuerdo con la entidad?	Sí-No
28. ¿En relación con la dirección, hay creación de uso de responsabilidades y roles?	Sí-No
29. ¿En relación con la dirección, hay comunicación de todo el personal que está involucrado en los indicadores de progreso y programa de mediciones?	Sí-No
30. ¿En relación con la dirección, se comprueba que el programa se lleva a cabo?	Sí-No
31. ¿En relación con la dirección, se establece el programa de mediciones?	Sí-No
32. ¿En relación con la dirección, se tienen los recursos suficientes para llevar a cabo el programa de mediciones?	Sí-No
NORMATIVA ISO/IEC 27004 – Parte 2	
1. En los objetivos de medición de la seguridad de la información en el contexto de SGSI, ¿se evalúa la eficacia de los controles aplicados o grupos de control?	Sí-No
2. En los objetivos de medición de la seguridad de la información en el contexto de SGSI, ¿se evalúa la eficacia de los sistemas de gestión de seguridad de la información implementado?	Sí-No
3. Los objetivos de medición de la seguridad de la información en el contexto	Sí-No

de SGSI, ¿se facilita la mejora del rendimiento de la seguridad de la información en cuantos a los riesgos de negocio?	
4. ¿En los objetivos de medición de la seguridad de la información en el contexto de SGSI, se verifica el grado en el que se fijaron las necesidades de seguridad y si han sido cumplidas?	Sí-No
5. ¿En los objetivos de medición de la seguridad de la información en el contexto de SGSI, se proporciona información para la revisión por parte de la dirección?	Sí-No
6. ¿El programa de la seguridad de información de la medición incluye medidas y medición de desarrollo?	Sí-No
7. ¿El programa de la seguridad de información de la medición incluye la operación de medición?	Sí-No
8. ¿El programa de la seguridad de información de la medición incluye el análisis de datos y medición de informar los resultados?	Sí-No
9. ¿El programa de la seguridad de información de la medición incluye la evaluación y mejora del programa de la seguridad de medición de la información?	Sí-No
10. ¿En los factores de éxito, hay compromiso por parte de la gerencia con el apoyo de los recursos apropiados?	Sí-No
11. ¿En los factores de éxito, hay existencia de procesos y procedimientos SGSI?	Sí-No
12. ¿En los factores de éxito, hay un proceso repetible capaz de capturar y presentar informes para proporcionar datos significativos?	Sí-No
13. ¿En los factores de éxito, hay medidas cuantificables sobre la base de objetivos SGSI?	Sí-No
14. ¿En los factores de éxito, hay datos fáciles de obtener que se pueden utilizar para la medición?	Sí-No
15. ¿En los factores de éxito, hay una evaluación de la efectividad de la seguridad de la información?	Sí-No
16. ¿En los factores de éxito, hay una evaluación de la efectividad de la medición de la aplicación de mejoras identificadas?	Sí-No
17. ¿En los factores de éxito, hay una aceptación de información sobre los resultados de medición de las partes interesadas?	Sí-No
18. ¿En la gestión de responsabilidades, la dirección establece objetivos para el programa de información de seguridad de medición?	Sí-No
19. ¿En la gestión de responsabilidades, la dirección establece una política para el programa de información de seguridad de medición?	Sí-No
20. ¿En la gestión de responsabilidades, la dirección establece las funciones y responsabilidades en materia del programa de información de seguridad de medición?	Sí-No
21. ¿En la gestión de responsabilidades, la dirección proporciona recursos suficientes para llevar a cabo las medidas?	Sí-No
22. ¿En la gestión de responsabilidades, la dirección asegura que los objetivos del programa de información de la seguridad de medición se cumplen?	Sí-No
23. ¿En la gestión de responsabilidades, la dirección establece el propósito de la medición para cada medida a construir?	Sí-No

24. ¿En el SGSI se examina su política?	Sí-No
25. ¿En el SGSI se examinan sus objetivos?	Sí-No
26. ¿En el SGSI se examinan sus controles?	Sí-No
27. ¿Se da prioridad a la información basada en los riesgos?	Sí-No
28. ¿Se da prioridad a las capacidades de la entidad?	Sí-No
29. ¿Se da prioridad a las políticas de seguridad?	Sí-No
30. ¿Se garantiza que los atributos seleccionados son apropiados para la medición?	Sí-No
31. ¿Se garantiza que hay un número de atributos suficientes para realizar la medición?	Sí-No
32. ¿El modelo de análisis está bien definido?	Sí-No
33. ¿Los indicadores están bien definidos?	Sí-No
34. ¿En la construcción de la medición contiene la información correspondiente al objeto de la medición?	Sí-No
35. ¿En la construcción de la medición contiene la información correspondiente al objetivo de control?	Sí-No
36. ¿En la construcción de la medición contiene la información correspondiente a los datos que se recogen y utilizan?	Sí-No
37. ¿En la construcción de la medición contiene la información correspondiente al proceso de recogida de datos y análisis?	Sí-No
38. ¿En la construcción de la medición contiene la información correspondiente al proceso para la representación de informes?	Sí-No
39. ¿En la construcción de la medición contiene la información correspondiente a las responsabilidades de las partes interesadas?	Sí-No
40. ¿Los datos se han obtenido dentro de los intervalos de tiempo?	Sí-No
41. ¿Los resultados de la medición son comunicados a los clientes?	Sí-No
42. ¿Los resultados de la medición son comunicados a los propietarios de la información?	Sí-No
43. ¿Los resultados de la medición son comunicados al personal responsable de las aéreas identificadas?	Sí-No
44. ¿El programa de medición de seguridad de la información produce resultados de medición de una manera eficaz?	Sí-No
45. ¿El programa de medición de seguridad de la información se ejecuta según lo previsto?	Sí-No
46. ¿El programa de medición de seguridad de la información se ejecuta según lo necesario?	Sí-No
47. ¿Los resultados de la medición son fáciles de entender?	Sí-No
48. ¿Los resultados de la medición son comunicados de manera oportuna?	Sí-No
49. ¿Los resultados de la medición son objetivos?	Sí-No
50. ¿Los resultados de la medición son comparables?	Sí-No
51. ¿Los resultados de la medición son útiles?	Sí-No
52. ¿Los resultados de la medición se corresponden con la necesidad de la información?	Sí-No
53. ¿Los procesos establecidos para el desarrollo de los resultados de medición están bien definidos?	Sí-No

54. ¿Los procesos establecidos para el desarrollo de los resultados de medición son fáciles de operar?	Sí-No
55. ¿Los procesos establecidos para el desarrollo de los resultados de medición son seguidos correctamente?	Sí-No

10.CONCLUSIONES

LO QUE HE APRENDIDO

Una vez terminado dicho proyecto he comprobado que no existe ni existirá una seguridad total capaz de defenderse de todos los ataques que ocurran tanto en el presente así como en un futuro cercano o lejano para la entidad, y por tanto la única meta que hay que aplicarse es la de la "mejora continua" ya sea mejorando los controles de seguridad tanto de los sistemas informáticos, como personales, etc.; hay que abarcar todo lo posible para reducir los futuros riesgos o amenazas venideras.

Incluso es necesario realizar pruebas sobre nuestro propio sistema mediante el uso de ataques intencionados, con el fin de comprobar nuestra propia seguridad, con el fin de estar preparados.

Además he conseguido tener una visión más concreta respecto a las normativas ISO/IEC se refiere.

He descubierto que "en el mundo de la ingeniería informática nunca se puede estar parado", siempre hay que mejorar y estudiar para los cambios, la ingeniería informática es una rama que evoluciona con el tiempo y que aquellos que se quedan atascados en el pasado no serán capaces de llegar a ningún lugar. Por lo tanto hay que aprende a evolucionar.

También gracias al proyecto he sido capaz de desempeñar una función como si de un trabajo real se tratase, documentándome, desarrollando, explicando, redactando, aplicando mis conocimientos de inglés para las documentaciones que no estaban en castellano. Así como la utilización de los conocimientos obtenidos a lo largo de estos años de carrera.

A lo largo de su realización he descubierto y aprendido que aunque tengamos un buen sistema de métricas en la seguridad informática no seremos capaces de buscar las respuestas a los problemas encontrados, en realidad lo que conseguimos es reducir en

cierto nivel ese agujero de seguridad que tendremos siempre, lo único que variara será el tamaño de dicho agujero y siempre tendremos que estar dispuestos a minimizarlo lo más posible, ya que es imposible eliminarlo por completo.

Además este proyecto me ha ayudado a obtener una mayor experiencia a la hora de alcanzar mis metas, en otras palabras "a buscarme la vida" con el fin de obtener los objetivos y resultados deseados.

APORTACIONES AL PROYECTO

En este proyecto he aportado la necesidad de las empresas a utilizar dicha normativa, siendo esta una piedra fundamental para la entidad a la hora de realizar su trabajo de forma correcta.

Así como también he explicado bastante información sobre dicha normativa.

Además de la situación en la que tiene que estar una empresa si quiere implantarla.

Por supuesto he añadido bastante información sobre las auditorías en este proyecto, he hablado sobre la auditoría informática, pero aun así en el anexo he englobado los diferentes tipos de auditorías que hay en el mundo del mercado laboral, lo cual también servirá de futura documentación a los interesados en estos temas de auditoría, porque existe una gran cantidad de auditorías que existen actualmente incluso pueden llegar a aparecer nuevas auditorías dependiendo de la necesidad de la entidad, por tanto el anexo servirá de gran ayuda a las generaciones venideras.

He realizado una serie de cuestionarios divididos en clases, los cuales ayudará a los procesos de auditoría para comprobar si el trabajo que están realizando en relación con la normativa ISO/IEC 27004, se está realizando de forma correcta, al igual que con los otros puntos de los cuestionarios, como seguridad física, seguridad lógica, acceso físico a la entidad, etc.

Además gracias a las cuestiones realizadas las personas que vengan detrás de mi podrán utilizarlo como un apoyo fundamental a la hora de la aplicación de tal normativa así como de su entendimiento.

También servirá de guía en relación a las entidades en el momento en el que deseen implantar una normativa. Con el fin de saber si dicha entidad está preparada para ello, en relación a sus características como empresa, hasta llegar al trato con el personal de la entidad.

VISION DE FUTUROS PROYECTOS

Podría recomendar buscar nuevos puntos de vista y mejoras a la normativa ISO/IEC 27004 la cual ha sido realizada creada hace poco tiempo y como todas con el paso de los años se descubrirán nuevos métodos y mediciones que todavía no se han creado, así como actualizaciones de dicha normativa y errores que pueden encontrar.

Este proyecto por tanto servirá de guía para futuros usuarios que deseen tener un conocimiento general y necesario para conocer dicha normativa y a partir de ella realizar las posibles mejoras.

Además a partir de dicha normativa podría crearse ciertas versiones centradas en otros puntos de seguridad en diferentes aéreas de la industria con el fin de expandirse.

La parte de seguridad física no está muy extendida y por tanto puede ser desarrollada por futuras generaciones de alumnos que utilicen este proyecto como guía.

El cuestionario con el paso de los años algunas preguntas podrán quedarse ambiguas con lo cual pueden ser actualizadas y ser mas exhaustivas

Además también servirá este proyecto como guía para explicar futuras normativas.

11. BIBLIOGRAFÍA

http://www.iec.ch/

http://www.agn.gov.ar/

https://www.agpd.es

http://www.icac.meh.es/

http://www.asesoriasygestorias.es/

http://www.isaca.org

http://www.iso.org

http://www.segu-info.com.ar

http://www.s21sec.com

http://www.wikipedia.org.

http://www.monografias.com/

Apuntes de la asignatura Auditoría Informática

ISO/IEC 27004 –Information technology – Security techniques- Information security management- Measurement

ISO 15408

ISO 27001 Information technology - Security techniques - Information security management systems - Requirements

Apuntes de la asignatura Seguridad y Protección de la Información.

Apuntes de la asignatura Gestión y Calidad del Software

http://www.rae.es

http://www.standardsinfo.net/

http://www.nist.gov/

http://www.uc3m.es/

http://www.secuware.com/

http://www.w3.org/WAI/

12.GLOSARIO

Back up: Es la copia total o parcial de información importante de bases de datos, CD´s, discos duros, etc.

Benchmarking: técnica utilizada por las empresas que consiste en la comparación con otras entidades con el fin de saber en qué se diferencian.

Costos: gasto económico de una entidad.

CPU: Central Processing Unit -Unidad de Proceso Central. Es donde se realizan los cálculos en los equipos informáticos.

E.R.E.: Expediente de Regulación de Empleo. Se trata de un procedimiento administrativo – laboral.

Firewall: Muro de Fuego - Cortafuego. Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

IP: (Internet Protocol - Protocolo de Internet). Protocolo para la comunicación en la red a través de paquetes conmutados.

Just-in-time: es un sistema de organización de la producción para las fábricas de origen japonés. El cual permite aumentar la productividad.

Hardware: componentes físicos que forman parte de un equipo informático (teclado, ratón, monitor,etc.)

Memoria RAM: Random Access Memory - Memoria de Acceso Aleatorio, es un chip en el cual se guardan, datos, programas que necesita el equipo informático y de forma temporal, cuando el equipo se apaga se pierde todo su contenido.

Mobbing: Acoso laboral que recibe el empleado por parte de su superior o por parte de sus compañeros de trabajo.

*Monitoreo 24*7*: Consiste en llevar un control de los equipos informáticos o aplicaciones durante 24 horas los 7 días de la semana.

SAI: Sistema de Alimentación Ininterrumpida. Cualquier dispositivo que permite dar energía eléctrica constante a un equipo informático incluso si el suministro principal de energía se ve interrumpido.

Seguridad Multinivel: la información es manejada de acuerdo a su nivel de sensibilidad y a los permisos que tiene la persona que desea acceder a ella

Software: grupo de programas para poder interactuar con el sistema.

Spyware: Software espía. Programa que recolecta información valiosa del equipo informático sin que el usuario lo sepa.

WAI: Web Accessibility Initiative. Iniciativa para la Accesibilidad Web. Vela por la accesibilidad de la web.

A.ANEXO

LA AUDITORÍA Y SUS CLASES

INDICE

1. Introducción

1.1 ¿Qué es la Auditoría?

Para empezar vamos a indicar una serie de definiciones sobre la Auditoría.

"Son una serie de técnicas y un grupo de procedimientos cuyo fin es evaluar y controlar un sistema con el objetivo de proteger sus recursos y activos, así como comprobar que las actividades que se realizan de forma eficiente y con la normativa general de cada empresa y para obtener la eficacia exigida en el marco de la organización estableciendo planes de acción y recomendaciones."

"Consiste en un examen detallado de la estructura de una empresa, en cuanto controles y métodos, su forma de operación, sus objetivos y planes, y sus equipos físicos y humanos".

" Es una visión sistemática y formal con el fin de determinar hasta que parte una organización cumple sus objetivos establecidos por la empresa, así como para diferenciar los que necesitan mejorarse"

"Es una función cuyo objetivo es apreciar y analizar, con vistas a las acciones correctivas eventuales, el control interno de la organización para cumplir la integridad del patrimonio, la autenticidad de la información así como el mantenimiento de la eficacia de los sistemas de gestión."

La auditoría es en sí una actividad que debe de realizar mediante el uso de conocimientos académicos, para ello se utiliza una serie de técnicas que nos lleven a la prestación de un servicio con alto nivel de calidad y reconociendo la responsabilidad social, no solo del cliente sino del público en general, que necesite hacer el uso del dictamen del auditor, para la elección de decisiones.

Clasificaciones de la auditoría.

Las clases que pueden llegar a dividir a la auditoría dependen, del requisito empresarial de instalar pautas o controles para el cumplimiento de las acciones que se realizan en la organización. Por ejemplo la auditoría operativa u administrativa se encarga de analizar

los materiales, recursos humanos, procedimientos, estructuras y programas de los diferentes complejos de la organización.

En resumen, las funciones que pertenecen a la gestión a excepción de la auditoría financiera, para comprobar su correcto funcionamiento, así como proponer nuevas mejoras así como la mejora de sus comportamientos disfuncionales.

Con lo explicado anteriormente nos aclara que la auditoría puede diferenciarse según sea su punto de aplicación, de igual manera podemos decir que se divide según sean sus objetivos

Bases Teóricas de una Auditoría.

La auditoría moderna está desarrollada en una serie de ideas que sirven para determinar cuál es la base fundamental de su aplicación. Los puntos son:

- La existencia de controles internos nos ayuda a disminuir la probabilidad de que se comentan en la organización fraudes irregulares.

- La auditoría está basada en que toda la información que se tiene puede ser verificada y comprobada.

- Si no se realizan pruebas, lo que fue verdad en el pasado volverá a serlo en el futuro. (Problemas que no se han solucionado, debidos a que no se han intentado resolver, no desaparecerán)

- Gracias a la auditoría evaluaremos y examinaremos las afirmaciones realizadas por los administradores, ya que puede ocurrir un intento de “tapar” afirmaciones las cuales podrían resultar embarazosas a los administradores

- No tiene porque existir un conflicto entre auditor y administrador de la organización que auditan.

Las normas de la auditoría

Normas Generales

- Hay que tener cuidado en la preparación del informe y el desarrollo de la auditoría.

- Para realizar una auditoría se necesita una persona o un grupo de personas que cuentan con la competencia del auditor y con una capacitación técnica adecuada.

- El auditor o los auditores tienen que tener una actitud mental de independencia.

Normas respecto a la Información

- Los informes contendrán una idea general y en referencia a los puntos que están involucrados en la auditoría. En el caso de que no se puede expresar una idea global, deberán de dar las causas de ello.

- Los informes nos avisarán si el área auditada o la información se presenta de una forma conforme con las bases o principios establecidos como guía de la auditoría

- Las elevaciones informativas se considerarán de forma razonablemente adecuada mientras que no se indique lo contrario.

Normas del Trabajo.

- Debe de ser planteado de forma adecuada y los asistentes estarán supervisados de una forma adecuada.

- Se tienen que conseguir evidencias competentes y suficientes mediante observaciones, inspecciones, consultas y confirmaciones, para tener una base lógica para tener una idea en referencia a la información obtenida o área que está siendo auditada.

1.2 Etapas de la auditoría general

Estudio General:

Está basado en la estimación general de las características de la empresa, de sus estados financieros y de sus elementos más importantes, de forma de que nos sirva para la orientación a la hora de aplicar una serie de técnicas que resulten más convenientes en la auditoría.

El concepto que debe de tener el auditor respecto del negocio del cliente es:

- Las condiciones Económicas y del Sector de la Empresa.

- La estructura de dicha Organización.

- Su estructura Legal y Operaciones.

Las condiciones Económicas y del Sector de la Empresa.

El auditor tendrá un conocimiento básico referente a las condiciones económicas de la empresa, así como las condiciones competitivas que llegan a afectar a las operaciones realizadas de un cliente y los cambios que se producen en la tecnología. La noción de las prácticas contables relacionadas en el sector de la industria en la cual el cliente se desenvuelve es de vital importancia.

La estructura de dicha Organización

En una organización de cualquier magnitud, será esencial el uso de un diagrama de la organización con el fin de especificar las tareas y las responsabilidades de los diversos miembros de la misma organización. La estructura de una asociación reparte las tareas entre los diversos empleados, las posiciones y departamentos o grupos. Para poder controlar el trabajo de una organización se adoptarán medidas de procedimiento y métodos que nos ayudarán a proporcionar evidencias de que aquellas tareas fijadas por la estructura de la asociación se llevan a cabo.

Su estructura Legal y Operaciones.

La auditoría comenzará con el conocimiento de las circunstancias y operaciones de la organización auditada. El auditor deberá de preparar una descripción breve de la naturaleza de aquellas actividades comerciales además de los factores más importantes que afectan a dichas operaciones.

Para ello el auditor deberá de tener un conocimiento referente a las características de funcionamiento, así como de los procedimientos relativos a la administración y de su estructura legal.

Para poder comprender la información obtenida mediante la auditoría, el auditor deberá de saber los negocios del cliente así como todos los factores que pueden llegar a influir en las operaciones

La revisión de los documentos legales de la organización es necesaria para el correcto entendimiento de los registros contables, y de sus estados financieros. Esta información nos ayudará a ampliar el conocimiento del negocio.

Hay que reconocer que sin esta fase del examen de la auditoría sería una restricción referente al alcance de esta área, en la cual sería una negativa por parte del cliente no permitir al auditor contemplar los libros de actas, lo que conducirá al auditor a la denegación de un dictamen. Ya que la información que se puede obtener de ello no se podrá obtener de otra forma.

Ejecución de la Auditoría

Encontraremos los aspectos siguientes en esta etapa:

- Análisis: nos ayudar a clasificar y agrupar elementos de la organización.

- Inspección: se trata de comprobar mediante una serie de pruebas los elementos de la organización.

- Confirmación: consistirá en obtener una comunicación por parte de una persona independiente de la empresa que está siendo auditada para el conocimiento de las condiciones y de la naturaleza de la operación de una manera válida sobre la misma

- Investigación: el auditor obtendrá una serie de conocimiento con el cual se formará un juicio sobre los elementos de la empresa por medio de datos, ya que estos nos sirven de base para la toma de decisiones.

- Observación: consiste en presenciar los hechos o ciertas operaciones, mediante las cuales el auditor se da cuenta de qué forma se realizan por el personal de dicha empresa.

Informe Final

El informe constará de dos partes la primera será de procedimiento y la segunda una opinión del auditor, con la primera parte se indicará el alcance de dicha auditoría mientras que la segunda será la opinión del autor referente al correcto funcionamiento y presentación de los estados de dicha organización.

El objetivo de este informe será dar una opinión independiente y profesional.

1.3 ¿Cuándo realizar una Auditoría y por qué?

Las razones más importantes a la hora de realizar una auditoría podrán ser algunas de las siguientes.

Razones Externas.

a) Cambio o modificación en el marco legislativo.

- La legislación o la liberación pueden cambiar el entorno, siendo este menos previsible ya que cambia la situación definida por las leyes reguladoras por otra regida por las fuerzas de otras entidades de la competencia.

- La anulación de barreras comerciales obligando la apertura de nuevos horizontes hacia mercados que pueden tener una competencia internacional en vez de los mercados internos cerrados.

- La privatización de las organizaciones puede cambiar la orientación de ellas mismas, obligando a pasar de un modelo burocrático a un modelo orientado a la eficiencia de las actuaciones y al servicio al cliente.

b) Fluctuaciones del mercado.

- La innovación y la mejora de la tecnología puede llegar a provocar que sectores industriales y las empresas queden obsoletas, para poder solucionar este problema deberán de adaptarse a los nuevos cambios

- Los ciclos económicos pueden llegar a obligar a ciertas organizaciones a adoptar a cambiar su orientación por lo cual tendrán que tener una serie de estrategias diferentes.

Razones interno-externas

a) La reorganización de una empresa

- Esto puede ser provocado por diferentes causas: ya sea un cambio de la propiedad de la empresa, creación de un producto nuevo, debilitamiento o desgaste en el equipo directivo así como un cambio en la estrategia.

b) Emisión de ofertas públicas en mercados

- Debido al éxito de una oferta pública, la publicidad de los resultados obtenidos de la auditoría puede llegar a servir para comunicar las ventajas competitivas de la empresa así como el destacar el talento de los gestores.

2. Tipos de Auditoría

Existen numerosos tipos de Auditorías de las cuales vamos a destacarlas y a continuación las trataremos de forma más detallada.

Entre las principales Auditorías tenemos las siguientes:

Contable (auditoría externa de estados financieros)	Revisa la contabilidad de los libros Y los registros contables de una organización
Energética	Análisis, inspección y estudio de los flujos de energía del edificio Sistema o proceso para comprender la energía dinámica del sistema bajo estudio
Informática	Determinar si se salvaguarda el activo empresarial, así como la integridad de los datos, utilización eficiente de sus recursos y llevar a cabo los fines de la organización
Medioambiental	Posición de forma medioambiental de la organización Y la cuantificación de sus logros
Social	Revisa la contribución a la sociedad así como la participación en actividades socialmente orientadas

Seguridad de Sistemas de Información	Gestión y análisis del sistema para corregir, detectar y prevenir las vulnerabilidades que pueden aparecer ya sea en redes, servidores, etc.
Innovación	Obtención de información de la entidad respecto a la innovación
Política	Revisión de actividades y procesos, orientadas ideológicamente, para toma de decisiones de un grupo
Accesibilidad	Comprobación de la accesibilidad de un lugar web mediante un experto
Marca	Nos sirve para medir el valor de la marca
Sarbanes-Oxley	Para las empresas que cotizan en bolsa de acuerdo a la ley Sarbanes-Oxley.

Código de Aplicaciones	Revisar código con el fin de encontrar errores en diseño y tiempo
Fiscal	Se dedica a observar el cumplimiento de las leyes fiscales.
Administrativa	Logros de los objetivos de la Administración. Desempeño de funciones administrativas.
Financiera	Veracidad de estados financieros. Preparación de informes de acuerdo a principios contables.
Operativa	Examina actividades y funciones dentro de una organización, considerando su personal, sistema, métodos, presupuestos y lugar que ocupa en la empresa

Nocturna	Se realiza a diario en los hoteles o restaurantes en el turno de noche, cuya función es chequear todas las cuentas.

2.1 Auditoría Contable

Las auditorías puede ser sobre cualquier tipo de actividad. Aparecen como la necesidad de la entidad de validar su información económica, mediante un servicio o empresa independiente. Cabe destacar que en las empresas grandes es normal la existencia de un departamento de auditoría interna, aunque hay que decir que también hay numerosas empresas dedicadas a la auditoría.

En referencia a las auditorías de estados Contables reside en un examen de la información contenida en estos por el auditor independiente al emisor. Con el fin de saber si los mismos fueron preparados de acuerdo a las normas contables existentes en cada región o país.

Realizados los procedimientos adecuados que se consideren oportunos por el auditor, deberá de dar una opinión de si los Estados Contables dan la realidad financiera y patrimonial del auditado. En cada punto dará una opinión desfavorable o favorable por parte de un Contador Público.

La auditoría contable (auditoría externa de estados financieros), consiste en un proceso llevado mediante unas normas, los estados financieros de una entidad se someterán a una verificación y un examen realizado por expertos independientes y cualificados (auditores), cuyo objetivo es que digan su opinión sobre la estabilidad que se merece la información económico-financiera contenida en los mismos. Esto se comunicará mediante el uso de un dictamen o informe de auditoría.

El objetivo de un examen de los estados financieros de una compañía, por parte de un auditor independiente, es la expresión de una opinión sobre si los mismos reflejan razonablemente su situación patrimonial, los resultados de sus operaciones y los cambios en la situación financiera, de acuerdo con los principios de contabilidad generalmente aceptados y con la legislación vigente.

La auditoría contable es útil e interesa a una variedad de organismos y personas por las siguientes razones:

- Garantiza el cumplimiento y la honestidad de la gestión llevaba a cabo. Los administradores y directivos querrán que se auditen o no dependiendo de que si quieren esconder algo o no, pero también varía según el gasto o coste de la auditoría

- Permite a los propietarios mostrarles la forma de cómo conserva su patrimonio incluyendo como se maneja y lo más importante el rendimiento obtenido.

- Consigue asegurarse de que la gestión, la dirección y el control del negocio se llevan de forma y de acuerdo con las políticas y procedimientos establecidos, permitiendo usar datos fiables a efectos de planificación y análisis.

- Gracias al informe obtenido del auditor servirá para tomar decisiones en función a la conveniencia de contratar créditos, distribuir dividendos, aumentar el capital, etc.

- El dictamen del auditor servirá como elemento de juicio para criticar la eficacia de la entidad.

- En algunos casos si no se está auditado no se puede entrar en bolsa.

- Sirve a los inversores ya que deberán obtener información de confianza que les permita conocer la situación financiera y rendimiento.

- Se realizan más auditorías cuando no coinciden propietario y accionista. Lo que en caso de problemas intentarán poner una solución.

Los principios básicos del control interno contable

Gracias a ciertos elementos que son esenciales para lograr un control interno correcto en la mayoría de las empresas son:

Con respecto a la organización:

- El número de empleados bajo el control de un jefe, supervisor, etc., permitiendo una efectiva supervisión.

- Separación de funciones entre áreas, personas o departamentos que llevan la ejecución, custodia, autorización, contabilización y pago o cobro de una transacción.

- Existencia de un área de auditoría interna la cual dependa de la gerencia, responsabilizándose de una continua evaluación, revisión y mejora del control interno

- Definición y explicación de líneas de autoridad y responsabilidad, a través de organigramas y de manuales de organización, etc.

Respecto a la ejecución, autorización y control de las operaciones:

- Uso de planes de cuentas normalizados.

- Uso de archivos seguros y apropiados.

- Instalación de controles para cumplir normas y procedimientos.

- Uso de cuentas de control y aplicación de cualquier otro procedimiento, para permitir la comprobación de la exactitud de la información contable.

- No puede existir ninguna persona que tenga la responsabilidad de todas las fases relacionadas con una operación.

- Utilización de procedimientos y normas operativos claramente definidos y a ser posible que aparezcan en manuales de procedimientos, flujo gramas, etc.

- Protección de los activos

- Uso del sistema de formularios con el fin de documentar de forma válida todas las operaciones de la compañía.

- Instalación de sistemas de seguros, de registro y operativos.

- Preparación de implantación y de presupuesto de sistemas de costes fiables.

Los siguientes principios pueden ser aplicados en la empresa:

- Implantación de procedimientos y normas mínimos.

- Selección de personal de calidad. Cualquier empresa necesita contratar personal de confianza y responsable para compensar la falta de controles que pudieran implantarse.

- Supervisión efectiva y directa de la gerencia. Importante en pequeñas empresas donde el sistema de eficacia del sistema depende de la supervisión de la gerencia.

Las pruebas de auditoría

Para realizar el examen es necesaria una serie de evidencias que se obtienen por medio de pruebas, que sirven para dar fiabilidad y validez a la información que se obtiene de los sistemas contables y de los estados financieros.

Estas evidencias son:

- Documental. Comprobación y verificación de documentos.

- Física. Para identificar la existencia de activos.

- Comparaciones y ratios. Comparaciones con la misma entidad pero en otra fecha, misma entidad otra sucursal.

- Registros contables. Sirven para la evidencia válida, resumen del proceso de contabilización de las operaciones realizadas por la compañía.

- Verbal. Uso de preguntas al personal de la empresa para descubrir hechos y acontecimientos concretos.

- Control Interno. Pruebas para comprobar el cumplimiento del sistema de control interno.

El auditor necesita realizar estas pruebas con el fin de obtener un informe detallado de la empresa.

2.2 Auditoría Energética

Consiste en un estudio, análisis e inspección de la energía que consume un edificio, sistema o proceso. Se lleva a cabo para reducir la cantidad de energía que consume el sistema sin afectar a la producción o servicios que la entidad ofrece al cliente.

Antes de la Auditoría (también conocido por auditoría de recorrido)

El proceso más rápido y simple en una auditoría. Consiste en una primera vista, que consiste en realizar un seguimiento por el edificio con el fin de identificar y familiarizarse con las zonas de desperdicio de energía, así como unos pequeños test con el fin de entender el proceso del personal. Sin embargo en este proceso solo se señalan los principales focos de pérdidas de energía, por lo tanto más adelante habrá que hacer una reseña también en las zonas de menor prioridad. Aun así, sabiendo cuales son las prioridades se hará una rápida estimación de costos, al igual del ahorro que se va a obtener. Cabe destacar que esto solo son unos preliminares y que no es lo suficiente para llegar a obtener una decisión final, ya que nos valdrán desde un principio de base para el desarrollo de la auditoría, la cual se hará más adelante y más detallada.

La Auditoría

Se realiza tomando como base el proceso anterior, ya que se toma la información sobre operación y la instalación. Se tomarán las facturas de los servicios públicos de hace desde 12 a 36 meses con el fin de que el auditor pueda evaluar la demanda de energía, la instalación y las tasas de energía. Si en estos se dispone de perfiles y datos detallados de energía servirán para analizar los signos de derroche energético. También se realizarán entrevistas ya pueden ser verbales o tipo test con el fin de obtener una información en profundidad con el personal de la entidad con el fin de comprender los mayores consumos de energía y sistemas para saber a corto y a largo plazo los patrones de consumo de energía. En esta auditoría además se obtendrá información más detallada sobre las zonas de menor prioridad con el fin de encontrar alguna solución, ya que solucionando pequeños problemas podremos obtener un gran ahorro.

Instalaciones que se comprobarán

Se comprobarán mediante el uso de equipo de medición, ya que es necesario medir para poder cuantificar el grado de calidad que tiene una instalación, los principales equipos que hay que comprobar serían los equipos de calefacción, climatización iluminación, eléctricos, hábitos de consumo y el aislamiento de todos los equipos

Realización de la auditoría

Este tipo de auditoría debemos de realizarla cuando no sabemos cuál es el consumo de nuestras instalaciones, cuando no se realiza un mantenimiento habitual de los equipos, los equipos utilizados no son eficientes o cuando se producen pérdidas de frío o calor al ser un aislamiento insuficiente o nulo.

2.3 Auditoría Informática

Sirve para recoger, agrupar y evaluar evidencias con el fin de confirmar si un sistema de información mantiene la integridad de los datos, salvaguarda el activo empresarial, cumple con los objetivos de la entidad de forma eficiente cumpliendo con las leyes y regulaciones establecidas.

Con esta auditoría podremos mejorar algunos puntos de la empresa como pueden ser la eficacia, seguridad, rentabilidad y eficiencia.

En este tipo de auditoría sus objetivos primarios son el control de la función informática, el análisis de los sistemas informáticos, que se cumpla la normativa en este ámbito y la revisión eficaz de la gestión de los recursos informáticos.

Pruebas en la auditoría

A lo largo de la auditoría se deben de realizar una serie de pruebas con el fin de obtener la mayor información posible a la hora de tomar decisiones

- Cumplimiento. Sirven para comprobar si un sistema de control interno funciona correctamente.

- Sustantivas. Se obtienen por observación, cálculos, entrevistas, muestreos, técnicas de exámenes analíticos, conciliaciones y revisiones. Sirven para verificar la integridad, exactitud y validez de la información.

- Clásicas. Se comprueban sistemas y aplicaciones con datos de prueba, en un entorno simulado. Observando la entrada y el resultado en la salida obtenido.

¿Cuando realizar la auditoría?

- Por deficiencias económicas, incrementos de los costes.

- Inseguridad en las instalaciones, ya sea seguridad física, lógica o la confidencialidad de los datos.

- Cuando hay mala imagen o no se cumple con la satisfacción de los clientes, debido a que no se reparan las averías en los plazos que deben de ser, cuando no se atiende correctamente a los clientes, o no se cumplen los plazos de entrega firmados.

- Deben de realizarse cuando se descubren problemas de descoordinación y desorganización, esto es debido a que no se cumplen los estándares de productividad conseguidos o cuando no coinciden los objetivos o no se cumplen con los de la compañía.

Objetivo de la auditoría informática

La operatividad consiste en que la entidad y las máquinas funcionen aunque sea mínimamente. Ya que no es necesario detener los equipos informáticos para descubrir sus fallos y comenzar de nuevo. Este tipo de auditoría se realizará cuando los equipos están operativos, en eso consiste su principal objetivo, que el hecho de realizar la auditoría no pare la productividad de la empresa totalmente. Para conseguir este objetivo habrá que realizar los siguientes controles.

- Controles Técnicos específicos, son necesarios para lograr la operatividad de los sistemas. Por ejemplo se puede descubrir que los parámetros de asignación automática en el espacio de un disco estén mal, provocando que no se pueda utilizar por otra sección distinta. Al igual que la pérdida de información provocando dificultad o anulando otras aplicaciones.

- Controles Técnicos Generales, sirven para comprobar la compatibilidad entre sistema operativo y software, así como la compatibilidad entre hardware y software. Y por tanto es de los más importantes, ya que un problema en la compatibilidad puede crear un gran problema en la entidad.

2.4 Auditoría Medioambiental

También conocida por Eco-auditoría. Este tipo de auditoría consiste en cuantificar la posición medioambiental de una entidad. El informe en esta auditoría ha de contener una posición medioambiental alcanzada así como una caracterización del desempeño. Esto puede ayudar para conseguir las necesidades pendientes para mejorar los indicadores de tales realizaciones y logros.

Esta auditoría surge por la preocupación por el medioambiente y la responsabilidad de las empresas ya que les concierne. Sirve para evaluar y dar unas bases a una política cuidadosa con el medioambiente, ya que rodea a las industrias.

Para analizar los riegos medioambientales que surgen debido a las actividades que realizan las industrias los cuales afectan al medio ambiente, se realizan auditorías para cumplir con la legislación vigente en cada país, sector de actividad o región.

Según pasa el tiempo se vuelven imprescindibles ya que en la mayoría de los casos la auditoría medioambiental resulta de obligado cumplimiento según sea la legislación.

Este tipo de auditorías pueden ser internas, dentro de la propia empresa, o externas realizadas por terceros.

Además son instrumentos de gestión que validan el funcionamiento correcto de las políticas adoptadas sobre el medio ambiente, las cuales ofrecen ventajas a la empresa como al medio ambiente.

Debe de haber un equilibrio entre desarrollo económico y conservación del medio ambiente.

Diferencias con otras auditorías

La mayor diferencia entre esta auditoría y el resto, es el carácter multidisciplinario de esta, ya que junta los esfuerzos de diferentes tipos de profesionales, ya sean técnicos, juristas y científicos. El equipo de trabajo debe de hacer un estudio del impacto medioambiental que provoca la entidad. Sus principales tareas serán investigación, evaluación, diagnósticos, dictamen y proposiciones en este orden. Dicho equipo estará formado por persona con conocimientos en estándares medioambientales además de técnicas para la reducción y minimización de impactos.

Ventajas de la auditoría medioambiental

Cabe destacar que el hecho de realizar este tipo de auditoría sirve para obtener una serie de ventajas en la entidad las cuales pueden ser.

-Facilidad para obtener seguros que puedan cubrir riesgos ambientales, como la obtención de permisos, ayudas, licencias, contratos públicos o subvenciones.

-Mayor rendimiento y utilización de recursos, consiguiendo un gran ahorro en la entidad.

-Sirve para una base de toma de decisiones debido a la información que se obtiene, lo que serviría para poder tomar nuevas estrategias.

Objetivos

El objetivo a cumplir en dicha auditoría consistirá en cumplir con la legislación vigente en materia medioambiental. Este es el principal problema que tienen las empresas a la hora de resolver sus conflictos por lo tanto se convierte en su principal objetivo, ya que al realizar dicha auditoría es porque no cumplen con las normas. Entonces en esta auditoría una vez realizada la investigación y realizado el informe final debe de proporcionar los medios necesarios para salvar la situación. Se realizará un plan de actuación para la entidad y además de que la empresa no vuelva a incumplir tal normativa.

2.5 Auditoría Social

Este tipo de auditoría constituye el proceso que una entidad realiza, para enseñar su balance de acción social, así como el comportamiento ético de la entidad u organización, en función de sus objetivos y a las personas directamente o indirectamente implicados.

La primera auditoría social que se realizó en España fue en Cataluña, para un proyecto de Europa.

Ventajas

Sus principales ventajas de esta auditoría son.

-Se obtiene un mayor rendimiento de los recursos humanos.

-Se refuerza la entidad cuando estamos ante cambios, consiste en involucrar a las personas que contribuyen en la entidad directamente o indirectamente con los valores de dicha entidad, incluyéndolos en proyectos y estrategias.

-Ayuda a la hora de toma de decisiones, la entidad tomará cualquier decisión difícil la cual pueda originar un beneficio a corto o a largo plazo para la empresa.

-Además nos ayuda a destacar el espíritu de la empresa y la aspiración de promocionar del personal.

La estrategia de la auditoría social

Nos servirá para evaluar y controlar las acciones tomadas por la empresa, para ello se aplicará la estrategia de recursos humanos con eficacia y coherencia, por tanto en un proceso estratégico hay que controlar, hacer un seguimiento y evaluar las acciones. Cabe destacar que los recursos humanos son un recurso de fuentes de ventajas y estratégico.

2.6 Auditoría de Seguridad de Sistemas de Información

Consiste en un estudio que abarca la gestión y el análisis para identificar y corregir las vulnerabilidades que se pueden encontrar en las estaciones de trabajo, servidores o redes de ordenadores. También cabe destacar que se puede dividir en auditoría física y lógica.

Obtenido el resultado, se detallan, archivan y reportan a sus responsables quienes tienen que tomar las medidas necesarias para establecer medidas preventivas de refuerzo.

Gracias a esto sabremos la situación exacta de sus activos de información respecto a protección, medidas de seguridad y control.

Áreas que abarca

En esta auditoría se llegan a abarcar las siguientes áreas de seguridad, ya que forman parte de los objetivos de una revisión de la seguridad.

- Las amenazas físicas externas

- La protección de datos según está fijado en la LOPD (Ley Orgánica de Protección de Datos) de cuyo Reglamento de Desarrollo destacamos el artículo 96 que consiste en que

"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas"

- Control de accesos adecuados físicos y lógicos

- Redes y comunicaciones: tipos de comunicaciones, protección de antivirus y las topologías.

- Desarrollo y uso de las políticas.

- Fundamentos de la seguridad: planes, políticas, funciones, etc.

- El desarrollo de aplicaciones en un entorno o lugar seguro.

- El control de producción

Cabe destacar que las áreas no son independientes unas a las otras ya que entre ellas tienen ciertos enlaces por los cuales están comunicadas unas a las otras.

Fases en la auditoría

Las fases que hay que hacer en este tipo de auditoría son las siguientes:

- Elección de objetivos así como su alcance y la profundidad de la auditoría.

- Recopilación de la información y el análisis de cualquier fuente que nos pueda servir.

- Uso de un plan de trabajo, además de los recursos y plazos necesarios para realizarlos.

- Aplicación de pruebas y de entrevistas.

- Análisis de resultados con su respectiva valoración de riegos.

- Presentación y las discusiones respecto al informe provisional.

- Informe final.

Auditoría de la seguridad física

Consistirá en la evaluación de las protecciones físicas de datos, equipos redes, programas instalaciones y soportes, además habrá que considerar a las personas, que estén protegidas y que haya medidas de evacuación, salidas alternativas, alarmas, etc.

Las amenazas pueden ser desde: vandalismo, explosiones, inundaciones, sabotaje, averías importantes, incendios, así como los demás que pueden afectar al trabajador impidiendo su trabajo afectando al funcionamiento correcto de la entidad como pueden ser huelgas, errores o negligencias.

Auditoría de la seguridad lógica

Habrá verificaciones para comprobar que cada usuario solo podrá acceder a los recursos los cuales autorice el propietario con las posibilidades que se hayan fijado, por ejemplo: lectura, borrado, modificación, ejecución, etc.

Se usaran métodos de autenticación, los cuales pueden ser desde la biometría el cual es uno de los más sofisticados hasta el método más usado que es la contraseña.

Las contraseñas cumplirán las normas y los estándares de la entidad. Algunos aspectos para evaluar en las contraseñas serán, una longitud mínima, un número de intentos para introducirla por el usuario, cambiarlas con el tiempo, etc.

2.7 Auditoría de Innovación

Consiste en obtener la información sobre la posición actual de la entidad frente a las innovaciones, comprobando si se llevan a cabo las actividades de este tipo, así como su desarrollo y los resultados obtenidos. El objetivo final de esta auditoría será una propuesta de las partes susceptibles de poder mejorar indicando el marco de actuación sobre ellas.

La innovación consiste en la mejora de los procesos productivos (mejorando la eficiencia disminuyendo los costes), uso de nuevas estructuras organizativas y la interacción y comunicación entre entidades, cambio en las formas del uso de los productos o nuevos servicios.

Metodología

Consiste en la evaluación de la capacidad innovadora que tiene una entidad, que gracias a ello sabemos la presión externa que tiene la entidad para innovar y como es la estructura de la entidad respecto a los procesos que tienen que ver con el desarrollo de las innovaciones para saber que procesos tienen que permanecer existiendo, cuales hay que incluir, cuales mejorar, su eficiencia y que herramientas se necesitan para realizarlo. Además de saber cuáles son las personas que participan en dicha evaluación, que pueden ser desde proveedores, clientes, etc. Obteniendo todo lo necesario que implica una función en la entidad.

Con ello se podrá analizar y evaluar la situación de los procesos de la entidad. Que están relacionados con la innovación, cómo mejorar, e introduciendo nuevos procesos, herramientas o mejoras para incrementar la capacidad innovadora, como por ejemplo:

-Uso de nuevas técnicas de creatividad.

-Toma de recolección, evaluación y selección de ideas nuevas.

- Comunicación con proveedores y clientes.

- Motivación de los empleados.

- Acuerdos o tratados de cooperación con empresas y universidades.

2.8 Auditoría Política

Consiste en una revisión detallada de las actividades y procesos, ideológicamente orientadas, de toma de decisiones de un grupo con el fin de obtener unos objetivos, en beneficios individuales y de grupo.

En dicha auditoría habrá que comparar, sistematizar, recompilar y evaluar los compromisos de campaña tomados por las personas que ocupan cargos de elección popular de un carácter público: congresistas, diputados, alcaldes, presidente regionales, presidentes de la nación, etc.; con las actividades realizadas una vez puestos en el cargo, así como los logros alcanzados en beneficio del pueblo.

2.9 Auditoría de Accesibilidad

Como su propio nombre indica consiste en la comprobación de la accesibilidad de una página web realizada por un experto. Terminada la auditoría se informará sobre los problemas que existen en dicha página respecto a su accesibilidad así mismo ofrecerá a la entidad posibles soluciones con el fin de arreglar el problema.

Tiene que cumplir con la Ley 34/2002 sobre la accesibilidad web.

Este tipo de auditoría sirve para que una página web pueda ser visualizada en cualquier tipo de soporte y lo más importante que sea visualizada también por usuarios discapacitados.

También hay otras técnicas para comprobar la accesibilidad y que no son de la auditoría de accesibilidad, son:

- Test Accesibilidad automático

- Test Accesibilidad

Ventajas

En referencia a estas dos técnicas la auditoría de accesibilidad se aventaja de ellas dos por el uso de menor coste económico, mayor rapidez y más exhaustivo a la hora de realizarlo.

Desventaja

En relación a estas dos técnicas su desventaja reside en que no se realiza una transmisión de conocimiento del auditor al cliente, el cual es quien está auditado con él.

Fases

Sus fases suelen ser:

- Se realiza una revisión preliminar. Consiste en un estudio del estado de la accesibilidad de la web de la entidad.

- Se hace una valoración de la accesibilidad de la página web respecto a las pautas de la WAI.

- Arreglo de problemas en la fase de desarrollo.

- Realización del informe.

- Monitorización constante y supervisión de cambios.

2.10 Auditoría de Marca

Nos sirve para saber el valor de una marca de una entidad mediante el uso de una métrica.

Con esta auditoría sabremos si la marca por la cual hacemos la auditoría se desempeña como se creía en un principio, ya sea para el dueño o el cliente a los cuales les afecta directamente la marca. Se puede realizar un análisis de la estrategia y de la experiencia de la marca con el fin de comprobar cómo se está comportando actualmente en el mercado.

También hay que reconocer que con este tipo de auditoría de marca se pueden obtener las diferencias que hay en la entidad construyendo un mapa para dar consistencia, además de obtener una visión universal de la marca por parte de toda la entidad.

No hay que olvidar que las marcas de las entidades están basadas en emociones humanas, y esto sirve para que las personas se sientan reconocidas con esa marca convirtiéndose en nuestros próximos clientes.

Gracias a esta auditoría podemos saber cuál es la posición de la marca mostrando como audiencias externas e internas perciben la fuerza del servicio. Explicamos en qué consiste cada una de ellas a continuación.

Auditoría de marca externa

Consiste en saber como la marca es percibida por gente de fuera de la entidad, ya sean clientes, proveedores, detallistas, etc. Consiste en analizarlos sobre como perciben la marca, basadas en sus experiencias pasadas. Que aunque la experiencia pasada no predice el futuro sí nos ayuda para hacernos una idea de cómo mejorar en ciertos puntos.

También cabe recalcar que se debe de incluir a los clientes perdidos así como distribuidores para obtener una información detallada de las razones por las cuales han decidido ir a la competencia. Toda la información obtenida es necesaria a la hora de realizar el informe final.

Auditoría de marca interna

Consiste en la toma de datos respecto a cómo valoran los empleados de la entidad mediante el uso de entrevistas o el uso de test, cualificando a la entidad en relación a la marca.

2.11 Auditoría Sarbanes-Oxley(auditoría de la bolsa)

Consiste en una revisión practicada a las firmas de las entidades que cotizan en la bolsa según la Ley Sarbanes-Oxley(SOX).

La Ley Sarbanes-Oxley, surge en 2002 con el objetivo de mejorar la protección de los accionistas respecto a las entidades que cotizan en bolsa según unas medidas. Esta ley llega a todo lo relacionado entre la entidad y la cotización en bolsa desde los directivos de las entidades, los analistas financieros o los consejos de administración.

Esta Ley se basa en seis puntos las cuales son los siguientes:

- Refuerzo de responsabilidades en el gobierno corporativo de las entidades.

- Auditores con mayor cualificación.

- Aumento de las sanciones debido a incumplimientos.

- Mejora de la supervisión respecto a los mercados cotizados.

- Mejora de la calidad de la información así como sus detalles.

- Obtener un comportamiento ético respecto a la información confidencial, que pueda afectar a la bolsa.

Estos puntos afectarán a la actividad del auditor a la hora de realizar dicha auditoría.

Ley Sarbanes-Oxley aplicada en la auditoría

Esta ley provoca la mejora de los sistemas de control interno financiero. Obligando a auditar a la entidad. Esta auditoría tiene como único objetivo mejorar la confiabilidad y la calidad de la información financiera mediante el uso de métricas con el fin de comprender los controles, riesgos, valoración identificación y prueba continua. La calidad de la información es uno de los puntos más importantes e influyentes ya que en la misma auditoría no se podrá obtener un informe correcto sobre el aspecto de la entidad que cotiza en bolsa si no se tienen unos datos detallados, correctos, condensados, completos y a tiempo. Además con esta ley se fijan estándares que deben de cumplir los auditores en dichas auditorías.

2.12 Auditoría de Código de Aplicaciones

Con esta auditoría conseguimos revisar el código de nuestros programas realizados para una aplicación con el fin de encontrar errores en el tiempo del diseño con el fin de mejorar nuestra calidad de nuestros productos

Este tipo de auditoría es necesaria del ciclo de vida del software en desarrollo, ya que si dejamos dicha revisión para el final lo que vamos a conseguir es que a la hora de arreglar dicho fallo sea mucho más costoso y se tardará mayor tiempo en arreglarlo, además con dicha auditoría minimizaremos el mantenimiento del código así como una mejora de la calidad, además conseguiremos que nuestro equipo de trabajo vaya obteniendo una mayor experiencia sobre cómo se deben realizar ciertas modificaciones.

Además los entornos integrados sirven para comprobar la sintaxis de nuestro código lo cual es una función necesaria pero su defecto es que no se encargan de ciertos puntos que pueden surgir en el código como puede ser la existencia del código duplicado, las convenciones de nombrado de las variables, la visibilidad innecesaria que puede haber de un atributo, o del conocido código muerto que consiste en un código el cual está escrito en la aplicación pero no se llega a usar nunca debido a que no es llamado.

Para solucionar estos problemas que pueden surgir usaremos las herramientas que tenemos en la auditoría de código de aplicaciones para solucionar dichos defectos que no podemos solucionarlos con los entornos integrados.

2.13 Auditoría Fiscal

Esta auditoría se puede definir de varias formas, así que pondremos a continuación algunas definiciones respecto a la auditoría fiscal.

"Proceso sistemático con el fin de evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre las actividades económicas así como otros acontecimientos relacionados, cuyo único objetivo consiste en determinar el grado de correspondencia del contenido informativo con las posibles evidencias que dieron lugar al origen, además de establecer si los informes entregados han sido elaborados observando los principios establecidos para el caso".

"Es una herramienta para la supervisión y control que sirve para la creación de una cultura de la disciplina de una organización que gracias a ella nos ayuda a descubrir vulnerabilidades que podemos encontrar en la entidad así como fallos en la estructura."

"Consiste en un examen de los comprobantes, cuentas, estados y anotaciones de la entidad".

Objetivos

Dividiremos sus objetivos en dos grupos, específicos y generales.

En el primer grupo tendremos que evaluar y revisar la efectividad, la aplicación y la propiedad de los controles internos, así como mejorar la eficiencia operacional, comprobar el grado de cumplimiento de las normas, procedimientos y políticas vigentes.

Mientras en el segundo grupo de objetivos consiste en comprobar el cumplimiento de los controles internos establecidos en la entidad, así como la comprobación de las cuentas de dicha organización desde un punto de vista contable, administrativo, operativo y financiero.

Hay que realizar ciertas funciones a la hora de aplicarse dicha auditoría.

- Comprobar y evaluar si existen posibles riesgos económico-fiscales, para poder reducirlos o evitarlos en el mejor de los casos.

- Imposición de multas debido a las infracciones fiscales que podemos encontrar a la hora de realizar dichas auditorías.

-Investigar cualquiera de los casos de denuncia y comisión de delitos fiscales.

-Presentarse a las reuniones semestrales con las administraciones locales y regionales que haya de auditoría fiscal competentes en las que participan en equipo con la Dirección General de la Auditoría Fiscal Federal, Jurídica de

Ingresos y de Recaudación en las que se evaluarán los avances y las acciones realizadas por, el Estado.

-Comprobar que existe una planificación fiscal la cual tiene que ser la más adecuada con respecto al entorno familiar y futuro de la propiedad.

Normas

Se exigirá una correcta planificación de los procedimientos y métodos a aplicar además de los necesarios papeles de trabajo cuyo objetivo será dar fundamentos a las conclusiones a la hora de realizar el examen final.

Hay que destacar que no todo el trabajo lo tiene que hacer el auditor ya que como tal deberá delegar ciertas acciones en ayudantes, pero no liberará al auditor de la responsabilidad del todo el trabajo.

Como definición de estas normas podemos decir que son los requisitos necesarios o mínimos de calidad relacionados con la personalidad del auditor, ya sea la información que da como resultado y la función que desempeña de este tipo de trabajo.

2.14 Auditoría Administrativa

Consiste en una revisión evaluatoria y sistemática de una organización, que se lleva a cabo con el fin de determinar si la entidad está operando de forma eficiente. Consiste en una búsqueda para encontrar los problemas y errores relacionados con la eficiencia dentro de la misma entidad. Esta auditoría tiene una revisión de los planes, objetivos y programas de la empresa; sus funciones y su estructura orgánica; sus sistemas, controles y procedimientos; las instalaciones de la entidad, el personal y el área en que se desarrolla, en función de la eficiencia de operación y el ahorro que se consigue en los costos. Además esta auditoría puede ser hecha por un licenciado en administración de empresas así como otros profesionales capacitados para dicha función. Gracias a esta auditoría conseguimos una opinión sobre la eficiencia administrativa de toda la entidad.

Principios

Al tratar este tipo de auditorías necesitamos explicar o recalcar tres principios fundamentales los cuales son los siguientes:

-El sentido de la evaluación. No se intenta evaluar la capacidad de contadores, abogados e ingenieros en las operaciones de sus trabajos. En realidad se ocupa de realizar una evaluación y examen de la calidad de la entidad tanto colectiva como individual, de las personas responsables (gerentes) de la administración de funciones de operación de dicha entidad y comprobar si se han llegado a tomar modelos necesarios que garanticen la implantación de los controles administrativos necesarios.

- La importancia del proceso de verificación. Habrá que determinar que se hace realmente en los niveles administrativos, operativos y directivos; gracias a la práctica nos indicará que ellos no siempre estarán de acuerdo con lo que el responsable del departamento o supervisor cree que está ocurriendo de verdad. Los procesos de esta auditoría respaldan técnicamente la comprobación mediante la observación directa, el análisis, la comprobación de información de terrenos así como la confirmación de datos.

-Capacidad de pensar en términos administrativos. El auditor en todo momento tendrá que saber colocarse en la posición de un administrador a quien se le hace responsable de dicha función operacional así como pensar como éste debería de hacer. Consiste en pensar de una forma administrativa.

Metodología y Fases

1. Objetivos y planes. Consiste en discutir y examinar con la dirección de la entidad el estado de los objetivos y los planes.

2. La Entidad.

2.1 Observar, estudiar y comprobar la estructura de la entidad respecto al área que se valora.

2.2 Comparar la estructura real de la entidad con la del pasado (estructura de hace un mes)

2.3 Comprobar si se llevan a cabo los principios de una buena entidad, departa mentalización y funcionamiento.

3. Prácticas y políticas. Realización de un estudio para saber qué acción hay que realizar con el fin de mejorar dichas prácticas y políticas.

4. Controles. Saber si estos son eficaces y adecuados para la entidad.

5. El equipo físico y su disposición. Saber si se pueden realizar mejoras en la disposición del equipo.

6. Reglamentos. Consiste en saber si la entidad cumple con los reglamentos federales, locales y estatales.

7. Procedimientos y sistemas. Comprobar si se encuentran irregularidades, errores o deficiencias en los objetos a examen y conseguir una solución para mejorarlos.

8. Personal. Saber cuáles son las necesidades de las personas de la entidad en relación al trabajo que están realizando.

9. Operaciones. Consiste en comprobar las operaciones con el fin de saber qué es lo que necesitan para obtener mejores resultados.

10. El informe. Se realizara un informe en el cual se mostrarán las deficiencias encontradas así como sus posibles soluciones.

2.15 Auditoría Financiera

Consiste en examinar los estados financieros así como las operaciones financieras mediante un examen sistemático de los registros y los libros de la entidad, con el fin de dar una opinión profesional.

Para ello esta auditoría contempla las transacciones que se han realizado en el pasado.

Dicha auditoría se puede definir de la siguiente manera:

"Consiste en el examen de los registros, comprobantes, documentos y otras evidencias que sustentan los estados financieros de una entidad u organismo, efectuado por el auditor para formular el dictamen respecto de la razonabilidad con que se presentan los resultados de las operaciones, la situación financiera, los cambios operados en ella y en el patrimonio; para determinar el cumplimiento de las disposiciones legales y para formular comentarios, conclusiones y recomendaciones tendientes a mejorar los procedimientos relativos a la gestión financiera y al control interno"

Objetivos

Los objetivos en esta auditoría se dividen en dos, los específicos y los generales.

-Específicos. Consisten en una serie de puntos los cuales son:

a. Examinar el manejo de los recursos financieros de una organización con el fin de establecer el grado en que sus servidores utilizan y administran los recursos y si la información financiera obtenida es útil, adecuada, oportuna y confiable.

b. Dar recomendaciones con el fin de mejorar el control interno y contribuir a la fortaleza de la gestión pública así como promover su eficiencia operativa.

c. Comprobar que las organizaciones realicen eficientes controles sobre los ingresos públicos, así como también comprobar las disposiciones reglamentarias, normativas y legales aplicables en las operaciones de las actividades desarrolladas.

d. Desarrollar los sistemas de informaciones de entes públicos, ya que sirven para la toma de decisiones así como la ejecución de la auditoría.

e. Cumplir y evaluar los objetivos establecidos para la prestación de servicios y la producción de bienes por los organismos de la administración pública.

-Generales. Su principal objetivo será dar un dictamen sobre la razonabilidad de los estados financieros preparados y organizados por la administración de las entidades públicas.

2.16 Auditoría Operativa

El concepto o definición de esta auditoría es la valoración independiente de todas las funciones y operaciones de una entidad, de una forma analítica objetiva y sistemática, para saber si se lleva a cabo. Procedimientos y políticas aceptables, además de comprobar si se mantienen las normas establecidas así como la utilización de los recursos de una forma económica y eficaz, también se debe saber si los objetivos y las metas de la entidad se han llegado a alcanzar.

Se basa en la consulta, revisión, investigación, comprobación, evidencia y verificación relacionada con la entidad. Consiste en un examen realizado por un personal independiente de acuerdo con normas de contabilidad, cuyo objetivo es dar una opinión que muestre lo acontecido en el negocio.

Objetivo

Su objetivo reside en identificar y comprobar las áreas de reducción de costes, intentar mejorar los procesos operativos y aumentar la rentabilidad con fines constructivos y de ayuda a las necesidades comprobadas o examinadas.

Con esta auditoría sabremos si la actividad que estamos comprobando puede operar de manera más efectiva, eficiente y económica. Además sirve para saber si la producción que se realiza en los departamentos cumple con las especificaciones dadas por la entidad. También nos ayudará a encontrar deficiencias en procedimientos, prácticas y políticas. Por último se revisará la financiación en la adquisición de productos y elementos para la realización de los productos o servicios de la entidad para determinar si afectan a la calidad y cantidad de compras que se hubieran realizado.

Metodología

La metodología de este tipo de auditoría está basada en 4 características.

- Familiarización. El auditor deberá conocer las metas de la entidad, además sobre cómo se van a conseguir y como van a determinar en los resultados obtenidos.

- Verificación. Hay que examinar una serie de muestras de transacciones, seleccionadas previamente por una muestra estadística. Al realizar dicha verificación se centrará en tres puntos concretos costo, calidad y periodo correcto.

- Recomendación y evaluación. Solo se podrán hacer cuando el auditor esté completamente seguro tras la realización del examen.

- Informar de los resultados obtenidos a la dirección. El resultado obtenido de hacer el informe deberá de ser entregado a los altos directivos.

2.17 Auditoría Nocturna

Es toda aquella que se realiza todos los días en el turno de noche, ya sean hoteles, cajeros o restaurantes.

Objetivo

Su objetivo es ayudar a la proporción y al desarrollo de los movimientos realizados durante el turno de noche, con el fin de ayudar al auditor de ingresos en su misión de elaborar, controlar y supervisar la contabilidad de la entidad (hotel).

Esta se realiza con la única finalidad de aligerar el trabajo del auditor de ingresos, debido a que el auditor nocturno tiene que realizar el cuadre de los ingresos obtenidos que se han tenido a lo largo de la noche para que así el auditor de ingresos pueda hacer la contabilidad más fácilmente.

Para ello el auditor nocturno deberá canalizar la operación de los cargos de los ingresos por ventas mientras que el auditor de ingresos hace la contabilización y la verificación de los ingresos del restaurante u hotel.

3. El Auditor

Para empezar tenemos que saber que un mismo auditor no tiene porque servir para distintas auditorías, por tanto tenemos que elegir aquella persona que tenga la experiencia necesaria y los conocimientos necesarios acorde al tipo de auditoría que se va a realizar ya que interactuará de una forma más natural.

Su formación académica puede ser desde unos estudios de nivel técnico hasta pasando por ingeniería industrial, derecho, informática, ciencias políticas, contabilidad, o cualquier otra formación, esto es debido a que las auditorías pueden ser de tantas clases como formaciones se tienen, lo importante es que tenga una formación relacionada con la auditoría que vaya a realizar, ya que por ejemplo un auditor en auditoría informática si el día de mañana va a realizar una auditoría fiscal y no tiene los conocimientos necesarios respecto a ese tema, no va a poder realizar el trabajo correctamente aunque su experiencia en auditorías sea alta .

También se valorará toda aquella formación complementaria que habrá obtenido el auditor mediante seminarios, conferencias o cursos de reciclaje.

Respecto a las características personales del auditor las cuales son determinantes a la hora de hacer su trabajo correctamente tiene que tener algunas de las siguientes propuestas a continuación:

-Estabilidad emocional: el auditor no podrá dejarse llevar por sentimientos personales (angustia, rabia, etc.) los cuales pueden influenciar negativamente a la hora de realizar dicha auditoría.

-Escuchar: deberá de estar atento y saber todo lo que está ocurriendo a su alrededor entendiendo claramente lo que diga el personal de la entidad.

-Analizar: tendrá que ser una persona capaz de examinar objetivamente una vez obtenidos los datos necesarios.

-Ética: tiene ser una persona con moral y que no se pueda corromper.

-Observador: tendrá que estar atento a todo lo que está pasando mientras realiza la auditoría.

-Optimista: habrá que dar una actitud positiva a la hora de realizar dicha auditoría para que la gente que esté en dicha entidad no llegue a tomarle miedo, aunque tendrán que demostrar cierto respeto al auditor.

-Objetivo: deberá de tener su propio punto de vista neutral a la hora de realizar el examen final.

-Discreción: su paso a la hora de realizar la auditoría desde la toma de datos hasta la realización del examen debe de pasar lo más inadvertido en la entidad.

-Trabajo en equipo: en el caso de trabajar con ayudantes u otros auditores deberá saber delegar el trabajo, así como una actitud correcta en todo el momento con los demás compañeros del equipo.

-Iniciativa: sabrá qué pasos realizar en cada momento y como tienen que hacerse sin dudar ni flaquear.

-Exposición en público: deberá expresarse correctamente al personal de la entidad.

Por último cabe resaltar que la experiencia del auditor es uno de los mayores puntos a favor que tiene, ya que gracias a ella cada vez tendrá mejores conocimientos y capacidades a la hora de enfrentarse a nuevos retos.